PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2002-164881**
(43)Date of publication of application : **07.06.2002**

(51)Int.Cl. **H04L 9/08**
G06F 13/00
G09C 1/00
H04L 9/32

(21)Application number : **2000-362913**
(22)Date of filing : **29.11.2000**

(71)Applicant : **SANYO ELECTRIC CO LTD**
FUJITSU LTD
PFU LTD
HITACHI LTD
NIPPON COLUMBIA CO LTD
(72)Inventor : **HORI YOSHIHIRO**
KAMIMURA TORU
HATAKEYAMA TAKAHISA
TAKAHASHI MASATAKA
TSUNEHIRO TAKASHI
OMORI YOSHIO

(54) DATA TERMINAL DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a data terminal device, which can move encrypted contents data and license distributed by software to other data terminal devices.
SOLUTION: A hard disc 530 in a personal computer has a contents list file 150 and an encrypted confidential file 160. A license management device 520 stores a binding key Kb into a license area 5215B of memory. The encrypted confidential file 160 can be decoded and encrypted by the binding key Kb stored in the license management device 520. The acquired license for the encrypted content data is stored in the encrypted confidential file 160 as confidential information.

CLAIMS

[Claim(s)]
[Claim 1]A license for decoding enciphered content data which enciphered contents data characterized by comprising the following, and said enciphered content data, and obtaining the original plaintext is acquired, A Data Terminal Equipment which outputs

said enciphered content data and said license to other Data Terminal Equipments.
A module part which acquires said enciphered content data and said license by software.
Said enciphered content data.
A license management file.
A binding key which decodes said encryption confidential file with a storage parts store which memorizes an encryption confidential file, and enciphers the decoded confidential file.

[Claim 2]At the time of initialization of said encryption confidential file, said module part, Said binding licenses including said binding key are generated, The Data Terminal Equipment according to claim 1 which gives said generated binding license to said device part while a **** confidential file is generated, and extra sensitive information enciphers the generated confidential file with said generated binding key and generates said encryption confidential file.
[Claim 3]At the time of acquisition of said license, said module part, It decodes with said binding key which acquired said encryption confidential file read from said storage parts store from said device part, Write said acquired license in the decoded confidential file as extra sensitive information, and said confidential file is updated, The updated confidential file is enciphered with said binding key, The Data Terminal Equipment according to claim 1 which carries out renewal record of the enciphered encryption confidential file to said storage parts store, creates a license management file containing a management number of extra sensitive information which makes a component said written-in license, and is written in said storage parts store.
[Claim 4]The Data Terminal Equipment according to claim 1 which said module part decodes said encryption confidential file read from said storage parts store with said binding key acquired from said device part, acquires a license at the time of transmission of said license, and outputs the acquired license to the exterior.
[Claim 5]The Data Terminal Equipment according to claim 4 which outputs said enciphered content data which said module part corresponded to said license, and was recorded on said storage parts store at the time of an output of said license, and said license to the exterior.
[Claim 6]The Data Terminal Equipment according to claim 1 which said device part receives an exclusive registration number which specifies said dedicated area from said module part, and stores said binding license in said dedicated area with the received exclusive registration number.
[Claim 7]The Data Terminal Equipment according to claim 6 which acquires said binding key at the time of an output of said license when said module part transmits said exclusive registration number to said device part.
[Claim 8]A Data Terminal Equipment given in any 1 paragraph of claim 1 to claim 7 which acquires said binding key when said module part transmits authentication data to said device part to said device part and said authentication data is attested in said device part at the time of an output of said license.
[Claim 9]A Data Terminal Equipment given in any 1 paragraph of claim 1 to claim 8 which said device part enciphers said binding key at the time of an output of said license, and is outputted.
[Claim 10]At the time of an output of said license, said module part, With said acquired binding key, decode said encryption confidential file and a confidential file is acquired, And the Data Terminal Equipment according to claim 4 which acquires a license outputted to the exterior by reading extra sensitive information which is in agreement with a management number of extra sensitive information included in a license management file read from said storage parts store from said acquired confidential file.

[Claim 11]At the time of transmission to other Data Terminal Equipments of said license, said module part, A Data Terminal Equipment given in any 1 paragraph of claim 1 to claim 9 which checks that writing of a binding license is possible for said device part by receiving an open encryption key held in said device part.
[Claim 12]At the time of movement to other Data Terminal Equipments of said enciphered content data, said module part, When a duplicate of said license is not made, extra sensitive information which makes a component a license which transmitted to a Data Terminal Equipment besides the above is deleted, The Data Terminal Equipment according to claim 10 which deletes a management number of the eliminated extra sensitive information, updates a license management file, generates another binding key, enciphers a confidential file and updates said encryption confidential file with the generated banding key of another.
[Claim 13]At the time of movement to other Data Terminal Equipments of said enciphered content data, said device part, The Data Terminal Equipment according to claim 11 which receives another binding license containing said another binding key from said module part, overwrites said dedicated area and stores the received binding license of another.
[Claim 14]A Data Terminal Equipment given in any 1 paragraph of claim 1 to claim 12 which will transmit a license to other Data Terminal Equipments if said module part attests authentication data received from a Data Terminal Equipment besides the above at the time of transmission to other Data Terminal Equipments of said license.
[Claim 15]The Data Terminal Equipment according to claim 13 outputted after said module part enciphers said license.
[Claim 16]A license for decoding enciphered content data which enciphered contents data characterized by comprising the following, and said enciphered content data, and obtaining the original plaintext is acquired, A Data Terminal Equipment which outputs said enciphered content data and said license to other Data Terminal Equipments.
A module part which acquires said enciphered content data and said license by software.
Said enciphered content data.
A license management file.
A storage parts store which memorizes an encryption confidential file which gave original encryption, and a binding key.

[Claim 17]At the time of initialization of said encryption confidential file, said module part, Said binding licenses including said binding key are generated, While generating a confidential file which stored the generated binding license, giving encryption original with the generated confidential file and generating said encryption confidential file, The Data Terminal Equipment according to claim 16 which gives said generated binding license to said device part.
[Claim 18]The Data Terminal Equipment according to claim 16 which said module part gives encryption original with said license, generates encryption extra sensitive information at the time of acquisition of said license, generates a license management file including the encryption extra sensitive information, and is written in said storage parts store.
[Claim 19]At the time of transmission of said license, said module part, If in agreement with a binding key with which said binding key acquired from said device part decoded and acquired said encryption confidential file, The Data Terminal Equipment according to claim 18 which decodes said encryption extra sensitive information read from said storage parts store, acquires a license, and transmits enciphered content data read from the acquired license and said storage parts store to other Data Terminal Equipments.
[Claim 20]The Data Terminal Equipment according to claim 16 which is the cipher

system related with information peculiar to a Data Terminal Equipment which can acquire said original cipher system from a Data Terminal Equipment.
[Claim 21]Said device part receives an exclusive registration number which specifies said dedicated area from said module part, The Data Terminal Equipment according to claim 16 which stores said binding license in said dedicated area and in which said module part generates said encryption confidential file and said license management files including said exclusive registration number with the received exclusive registration number.
[Claim 22]The Data Terminal Equipment according to claim 21 which acquires said binding key at the time of transmission of said license when said module part transmits said exclusive registration number to said device part.
[Claim 23]At the time of transmission to other Data Terminal Equipments of said license, said module part, A Data Terminal Equipment given in any 1 paragraph of claim 16 to claim 23 which acquires said binding key when authentication data to said device part is transmitted to said device part and said authentication data is attested in said device part.
[Claim 24]A Data Terminal Equipment given in any 1 paragraph of claim 16 to claim 23 which will transmit a license to other Data Terminal Equipments if said module part attests authentication data received from a Data Terminal Equipment besides the above at the time of transmission to other Data Terminal Equipments of said license.
[Claim 25]A Data Terminal Equipment given in any 1 paragraph of claim 1 to claim 24 in which said module part acquires said enciphered content data and said license from a distributing server by the Internet.
[Claim 26]Have further a medium actuator which reads contents data of a plaintext from a recording medium, and said module part, A license is generated based on duplicate propriety information included in contents data which said medium actuator read, A Data Terminal Equipment given in any 1 paragraph of claim 1 to claim 24 which acquires said enciphered content data and said license by enciphering said contents data and generating enciphered content data with a license key contained in the generated license.
[Claim 27]Further, said device part receives said enciphered content data and a license from a distributing server, holds the received license, and said storage parts store, A Data Terminal Equipment given in any 1 paragraph of claim 1 to claim 24 which memorizes enciphered content data received by said device part.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention relates to the Data Terminal Equipment used in the data distribution system which makes copyright protection to the copied information possible.
[0002]
[Description of the Prior Art]Each user is able to access network information easily in recent years with the terminal for the individuals [progress / of information-and-telecommunications networks, such as the Internet, etc.] using a reproduction terminal etc.
[0003]In such an information-and-telecommunications network, information is transmitted by a digital signal. Therefore, it is possible to perform a copy of data, without producing most degradation of the tone quality by such a copy, or image quality, even when an individual user copies the music and picture image data which were

transmitted, for example in the above information-and-telecommunications networks.
[0004]Therefore, if the policy for suitable copyright protection is not taken when the creation thing in which the right of authors, such as music data and image data, exists in such an information-and-telecommunications screen oversize is transmitted, there is a possibility of infringing on right of an owner of a copyright remarkably.
[0005]On the other hand, supposing it cannot give top priority to the purpose of copyright protection and cannot distribute work data via the digital information communications network to expand rapidly, it will become rather disadvantageous also for the owner of a copyright who can collect a fixed royalty when reproducing work data fundamentally.
[0006]If it thinks and sees here not taking the case of distribution through the above digital information communications networks but taking the case of the recording medium which recorded digital data, Usually, about CD (compact disk) which recorded the music data currently sold, the copy of the music data from CD to magneto-optical discs (MD etc.) can be freely performed in principle, as long as the copied music concerned is stopped to individual use. However, the individual user who performs digital sound recording etc. is to pay an owner of a copyright indirectly the constant sum of the prices for media, such as digital-sound-recording apparatus itself and MD, as a royalty.
[0007]And when the music data which is a digital signal is copied to MD from CD, It has come to be unable to perform copying to MD of further others as music data from recordable MD on the composition of apparatus in view of these information being the digital data which does not almost have copy degradation for copyright protection.
[0008]Since distributing music data and image data to the public through a digital information communications network also from such a situation is an act from which itself receives restriction by rights of public transmission of an owner of a copyright, sufficient policy for copyright protection needs to be devised.
[0009]In this case, it is necessary for the contents data received once to prevent being reproduced still more freely or being used even if it can reproduce about the contents data of music data, image data, etc. which is works transmitted to the public through an information-and-telecommunications network.
[0010]Then, the data distribution system with which the distributing server holding the enciphered content data which enciphered contents data distributes enciphered content data via a terminal unit to the memory card with which terminal units, such as a reproduction terminal, were equipped is proposed. In this data distribution system, the open encryption key and certificate of the memory card beforehand attested by the certificate authority are transmitted to a distributing server in the case of the distribution request of enciphered content data, After checking having received the certificate in which the distributing server was attested, the license key for decoding enciphered content data and enciphered content data to a memory card is transmitted. And when distributing enciphered content data and a license key, a distributing server and a memory card generate a different session key for every distribution, with the generated session key, encipher an open encryption key and exchange keys a distributing server and between memory cards.
[0011]Eventually, a distributing server transmits the license which it was enciphered with the open encryption key of memory card each, and was further enciphered with the session key, and enciphered content data to a memory card. And a memory card records the license and enciphered content data which were received on a memory card.
[0012]And a portable telephone is equipped with a memory card when reproducing the enciphered content data recorded on the memory card. A portable telephone also has a dedicated communication circuit for decoding the enciphered content data from a

memory card other than the usual telephone function, and reproducing, and outputting to the exterior.
[0013]Thus, the user of a portable telephone can receive enciphered content data from a distributing server using a portable telephone, and can reproduce the enciphered content data.
[0014]On the other hand, distributing enciphered content data to a personal computer using the Internet is also performed. And although it is possible to distribute the enciphered content data to a personal computer and a license in a similar way, Distribution of enciphered content data and a license is received by the software installed in the personal computer, moving the enciphered content data and the license which protection of the license is performed and were received to other personal computers -- RA from a viewpoint of copyright protection -- **** -- it is not divided.
[0015]That is, cipher processing related with values, such as an identification number etc. of BIOS which is the identification number and boot program which were individually given to CPU of the personal computer which recorded the license distributed to the personal computer, is used, Even if it copies to other personal computers then, a license cannot be taken out but the managing structure which carries out enciphered content decoding and cannot be reproduced is adopted. And supposing it provides the service which can move a license to other personal computers under this management, on a recorder, Although a license cannot be specified, by service which manages enciphered content data and a license, backups all the data currently recorded, and was provided. After moving enciphered content data and a license to other personal computers, The enciphered content data and the license which backupped will be managed, and it will be the same as could reproduce the state before movement, when returning all the data currently recorded to the personal computer, and having reproduced enciphered content data and a license. In movement of the license in such management, a security hole exists clearly. Therefore, the enciphered content data and the license which were distributed to the personal computer by software are to be moved to other personal computers.
[0016]
[Problem(s) to be Solved by the Invention]However, from the personal computer, entirely, supposing it cannot take out the enciphered content data and the license which were distributed to the personal computer, When CPU is changed by breakage of a personal computer, and upgrade, there is a problem that the enciphered content data and the license which were already received cannot be used.
[0017]then, this invention is made in order to solve this problem, and it comes out. The purpose is to provide a movable Data Terminal Equipment for the enciphered content data and the license which were distributed as be alike to other Data Terminal Equipments.

[0018]
[The means for solving a technical problem and an effect of the invention] The Data Terminal Equipment by this invention acquires the license for decoding the enciphered content data and enciphered content data which enciphered contents data, and obtaining the original plaintext, The module part which is a Data Terminal Equipment which outputs enciphered content data and a license to other Data Terminal Equipments, and acquires enciphered content data and a license by software, The storage parts store which memorizes enciphered content data, a license management file, and an encryption confidential file, It has a device part which stores in a dedicated area the binding license containing the binding key which decodes an encryption confidential file and enciphers the decoded confidential file, A license management file contains the management

number of the extra sensitive information which corresponds to an encryption contents file and is included in a confidential file including the extra sensitive information to which a confidential file makes a license a component.
[0019]In a Data Terminal Equipment by this invention, a module part, Enciphered content data and a license are acquired with software, It writes in a confidential file which decoded an encryption confidential file with a binding key taken out from a device part, and decoded an acquired license, and with a binding key, a confidential file is enciphered and an encryption confidential file is generated. That is, a module part manages a license which opened, closed and acquired an encryption confidential file via a binding key held by hardware in a device part.
[0020]Therefore, a license for according to this invention, decoding enciphered content data acquired by software, and reproducing, Since it is managed with a binding key held at hardware, enciphered content data and a license which were acquired are movable to other Data Terminal Equipments.
[0021]At the time of initialization of an encryption confidential file, preferably a module part of a Data Terminal Equipment, While binding licenses including a binding key are generated, and extra sensitive information enciphers with a binding key which generated a **** confidential file and generated the generated confidential file and generates an encryption confidential file, A generated binding license is given to a device part.
[0022]At the time of initialization of an encryption confidential file, a module part, While generating a binding license containing a binding key and a **** confidential file, enciphering a confidential file with a binding key and generating an encryption confidential file, a binding license is held to a device part.
[0023]Therefore, according to this invention, a confidential file which stores a license of enciphered content data acquired with software is created in soft, and a binding license for managing that created confidential file can be managed in hard.
[0024]At the time of acquisition of a license, preferably a module part of a Data Terminal Equipment, It decodes with a binding key which acquired an encryption confidential file read from a storage parts store from a device part, Write in a license acquired to the decoded confidential file as extra sensitive information, and a confidential file is updated, The updated confidential file is enciphered with a binding key, a license management file containing a management number of extra sensitive information which makes a component a license which carried out renewal record of the enciphered encryption confidential file to a storage parts store, and wrote it in is created, and it writes in a storage parts store.
[0025]A license which opened, closed and acquired an encryption confidential file with a binding key acquired from a device part is written in a confidential file. And license management files including a management number of extra sensitive information which makes a component the written-in license are created.
[0026]Therefore, according to this invention, a license of enciphered content data acquired in soft is manageable with a management number.
[0027]Preferably, at the time of transmission of a license, with a binding key acquired from a device part, a module part of a Data Terminal Equipment decodes an encryption confidential file read from a storage parts store, acquires a license, and outputs the acquired license to the exterior.
[0028]With a binding key acquired from a device part, a module part decodes an encryption confidential file, acquires a license, and outputs the acquired license to the exterior.
[0029]Therefore, according to this invention, a license of enciphered content data acquired in soft is movable to other devices like a license of enciphered content data

acquired in hard.
[0030]Preferably, a module part of a Data Terminal Equipment outputs to the exterior enciphered content data and a license which were equivalent to a license and were recorded on a storage parts store at the time of an output of a license.
[0031]At the time of an output to the exterior of a license, enciphered content data corresponding to a license taken out from a confidential file is read from a storage parts store, and enciphered content data and a license are outputted to the exterior.
[0032]Therefore, according to this invention, enciphered content data and a license are read in soft, and enciphered content data and a license can be moved to other devices.
[0033]Preferably, a device part of a Data Terminal Equipment receives an exclusive registration number which specifies a dedicated area from a module part, and stores a binding license in a dedicated area with the received exclusive registration number.
[0034]A device part stores a binding license for opening and closing an encryption confidential file via an exclusive registration number in a dedicated area.
[0035]Therefore, according to this invention, a binding license and a license of enciphered content data can be matched with an exclusive registration number.
[0036]Preferably, a module part of a Data Terminal Equipment acquires a binding key by transmitting an exclusive registration number to a device part at the time of an output of a license.
[0037]A module part acquires a binding key for opening a confidential file in which a license to read from a storage parts store was stored via an exclusive registration number.
[0038]Therefore, according to this invention, a binding key is correctly acquirable with an exclusive registration number.
[0039]Preferably, a binding key is acquired, when a module part of a Data Terminal Equipment transmits authentication data to a device part to a device part and authentication data is attested in a device part at the time of an output of a license.
[0040]A binding key is given only to an attested module part. Therefore, according to this invention, an outflow of an inaccurate binding key can be prevented.
[0041]Preferably, a device part of a Data Terminal Equipment enciphers and outputs a binding key at the time of an output of a license.
[0042]A device part enciphers and outputs a binding key for managing a license.
[0043]Therefore, according to this invention, when moving a license to other devices, a binding key which manages a license in a movement destination is made that it is hard to be acquired unjustly.
[0044]At the time of an output of a license, preferably a module part of a Data Terminal Equipment, With an acquired binding key, decode an encryption confidential file and a confidential file is acquired, And a license outputted to the exterior is acquired by reading from a confidential file which acquired extra sensitive information which is in agreement with a management number of extra sensitive information included in a license management file read from a storage parts store.
[0045]A module part acquires a binding key from a device part, decodes an encryption confidential file and acquires a license which is going to acquire extra sensitive information which is in agreement with a management number from extra sensitive information included in the decoded confidential file, and it is going to output to the exterior.
[0046]Therefore, according to this invention, a license is correctly acquirable via a management number.
[0047]When a module part of a Data Terminal Equipment receives preferably an open encryption key held in a device part further at the time of transmission to other Data Terminal Equipments of a license, a device part checks that writing of a binding license

is possible.
[0048]A module part is checked by receiving an open encryption key for whether it is a device part which can write in a binding license of a device part from a device part at the time of transmission to other devices of a license.
[0049]Therefore, according to this invention, when a license of enciphered content data is moved, it can recognize having moved a license by rewriting a binding license stored in a device part.
[0050]At the time of movement to other Data Terminal Equipments of enciphered content data, preferably a module part of a Data Terminal Equipment, When a duplicate of a license is not made, extra sensitive information which makes a component a license which transmitted to other Data Terminal Equipments is deleted, A management number of the eliminated extra sensitive information is deleted, a license management file is updated, another binding key is generated, with the generated banding key of another, a confidential file is enciphered and an encryption confidential file is updated.
[0051]When a duplicate of a license which moved is forbidden, a module part generates another binding key and updates an encryption confidential file while deleting a license which moved.
[0052]Therefore, according to this invention, a license can be prevented from being reproduced unjustly.
[0053]At the time of movement to other Data Terminal Equipments of enciphered content data, preferably a device part of a Data Terminal Equipment, Another binding license containing another binding key is received from a module part, a dedicated area is overwritten and the received binding license of another is stored.
[0054]When another binding key is generated, rewriting of a binding license is performed in a device part.
[0055]Therefore, according to this invention, a license for reproducing enciphered content data according to the newest binding license is manageable.
[0056]Preferably, attestation of authentication data which a module part of a Data Terminal Equipment received from other Data Terminal Equipments at the time of transmission to other Data Terminal Equipments of a license will transmit a license to other Data Terminal Equipments.
[0057]A module part transmits a license of enciphered content data, after checking that a Data Terminal Equipment which is going to move a license of enciphered content data is a regular terminal unit.
[0058]Therefore, according to this invention, a license of enciphered content data can be moved between regular Data Terminal Equipments, and enciphered content data can fully be protected.
[0059]Preferably, a module part of a Data Terminal Equipment is outputted after enciphering a license.
[0060]A module part moves to other Data Terminal Equipments, after enciphering a license.
[0061]Therefore, according to this invention, it is hard to acquire that license unjustly at the time of movement of a license.
[0062]A Data Terminal Equipment by this invention acquires a license for decoding enciphered content data and enciphered content data which enciphered contents data, and obtaining the original plaintext, A module part which is a Data Terminal Equipment which outputs enciphered content data and a license to other Data Terminal Equipments, and acquires enciphered content data and a license by software, A storage parts store which memorizes enciphered content data, a license management file, and an encryption confidential file that gave original encryption, A confidential file which was provided with a device part which stores in a dedicated area a binding license containing a

binding key, and decoded an encryption confidential file, A license management file includes encryption extra sensitive information which gave encryption original with extra sensitive information which corresponds to enciphered content data and makes a license a component including the same binding license as a binding license which a device part stores.
[0063]In a Data Terminal Equipment by this invention, a module part, By software, enciphered content data and a license are acquired, encryption original with the acquired license is given, encryption extra sensitive information is generated, a license management file including the generated encryption extra sensitive information is created, and it writes in a storage parts store. A binding license which manages a license is stored in a confidential file.
[0064]Therefore, according to this invention, since a binding key for managing a license is held by hardware, it can move a license for decoding enciphered content data acquired by software and reproducing to other Data Terminal Equipments.
[0065]At the time of initialization of an encryption confidential file, preferably a module part of a Data Terminal Equipment, Generate binding licenses including a binding key and a confidential file which stored the generated binding license is generated, While giving encryption original with the generated confidential file and generating an encryption confidential file, a generated binding license is given to a device part.
[0066]A module part generates a binding license containing a binding key and a **** confidential file at the time of initialization of an encryption confidential file, While writing in a binding license generated to a confidential file, performing original encryption and generating an encryption confidential file, a binding license is held to a dedicated area of a device part.
[0067]Therefore, according to this invention, since a binding key for managing a license is held by hardware, it can move a license for decoding enciphered content data acquired by software and reproducing to other Data Terminal Equipments.
[0068]Preferably, at the time of acquisition of a license, a module part of a Data Terminal Equipment gives encryption original with a license, generates encryption extra sensitive information, generates a license management file including the encryption extra sensitive information, and writes it in a storage parts store.
[0069]A module part gives encryption original with an acquired license, and manages it by a storage parts store.
[0070]Therefore, according to this invention, a license is manageable with an original cipher system.
[0071]At the time of transmission of a license, preferably a module part of a Data Terminal Equipment, If in agreement with a binding key with which a binding key acquired from a device part decoded and acquired an encryption confidential file, Encryption extra sensitive information read from a storage parts store is decoded, a license is acquired, and enciphered content data read from the acquired license and storage parts store is transmitted to other Data Terminal Equipments.
[0072]A module part is restricted when a binding key stored in a device part and a binding key stored in a storage parts store are in agreement, and it acquires a license.
[0073]Therefore, only a module part which has the same binding key as a binding key managed in hard can acquire a license.
[0074]A desirable original cipher system is a cipher system related with information peculiar to a Data Terminal Equipment acquirable from a Data Terminal Equipment.
[0075]A module part enciphers a license with a cipher system based on information peculiar to a Data Terminal Equipment, for example, a version number of CPU, etc.
[0076]Therefore, according to this invention, even if an enciphered license flows into

other devices unjustly, that license is not acquired unjustly.
[0077]Preferably a device part of a Data Terminal Equipment, Receiving an exclusive registration number which specifies a dedicated area from a module part, with the received exclusive registration number, a binding license is stored in a dedicated area and a module part generates an encryption confidential file and license management files including an exclusive registration number.
[0078]A device part manages a binding license in hard with an exclusive registration number generated by module part, and a module part enciphers uniquely and manages a generated exclusive registration number and an acquired license in soft.
[0079]Therefore, according to this invention, a module part acquires a binding key held via an exclusive registration number at a device part, and can distinguish correctly coincidence with a binding key read from an encryption confidential file, and a binding key acquired from a device part.
[0080]Preferably, a module part of a Data Terminal Equipment acquires a binding key by transmitting an exclusive registration number to a device part at the time of transmission of a license.
[0081]A module part transmits an exclusive registration number to a device part, and a device part takes out and outputs a binding key from a dedicated area specified with a received exclusive registration number.
[0082]Therefore, according to this invention, a binding key is correctly acquirable with an exclusive registration number.
[0083]A binding key is acquired, when authentication data [as opposed to / time of transmission to other desirable Data Terminal Equipments of a license / a device part in a module part of a Data Terminal Equipment] is transmitted to a device part and authentication data is attested in a device part.
[0084]Only when justification to a device part of a module part is checked, a module part acquires a binding key.
[0085]Therefore, according to this invention, a license can be prevented from being able to prevent unjust acquisition of a binding key and as a result being unjustly moved to other terminal units.
[0086]Preferably, attestation of authentication data which a module part of a Data Terminal Equipment received from other Data Terminal Equipments at the time of transmission to other Data Terminal Equipments of a license will transmit a license to other Data Terminal Equipments.
[0087]If it is checked that a Data Terminal Equipment which is going to move enciphered content data and a license is regular, a module part will transmit enciphered content data and a license to other Data Terminal Equipments.
[0088]Therefore, according to this invention, movement of enciphered content data and a license is possible only between regular Data Terminal Equipments.
[0089]Preferably, a module part of a Data Terminal Equipment acquires enciphered content data and a license from a distributing server by the Internet.
[0090]Therefore, according to this invention, contents data which acquired various kinds of contents data, and was acquired to other terminal units is movable.
[0091]Preferably, a Data Terminal Equipment is further provided with a medium actuator which reads contents data of a plaintext from a recording medium, and a module part, A license is generated based on duplicate propriety information included in contents data which a medium actuator read, Enciphered content data and a license are acquired by enciphering contents data and generating enciphered content data with a license key contained in the generated license.
[0092]A Data Terminal Equipment acquires enciphered content data and a license by ripping.

[0093]Therefore, according to this invention, contents data distributed by means other than a means of communication is also acquired, and it can move to other Data Terminal Equipments.
[0094]Preferably, further, a device part of a Data Terminal Equipment receives enciphered content data and a license from a distributing server, and holds the received license, and a storage parts store memorizes enciphered content data received by device part.
[0095]A device part receives enciphered content data and a license from a distributing server, and holds the received license with a binding license while it holds a binding license.
[0096]Therefore, according to this invention, a license acquired by hardware and a license acquired by software are manageable with the almost same security level.
[0097]
[Embodiment of the Invention]It explains in detail, referring to drawings for an embodiment of the invention. Identical codes are given to a portion same in the inside of a figure, or considerable, and the explanation is not repeated.
[0098][Embodiment 1] While the Data Terminal Equipment (personal computer) by this invention acquires enciphered content data, drawing 1, It is a schematic diagram for explaining notionally the entire configuration of the data distribution system which moves the acquired enciphered content data to other Data Terminal Equipments (personal computer).
[0099]Although digital music data is explained taking the case of the composition of the data distribution system distributed to the user of each personal computer via the Internet below, When distributing the contents data as other works, for example, image data, dynamic image data, etc., this invention can be applied without being limited in such a case, so that it may become clear by the following explanation.
[0100]With reference to drawing 1, the personal computer 50 transmits the distribution request (distribution request) from the user of each personal computer to the distributing server 10 via the modem 40 and Internet network 30. The distributing server 10 which manages the music data in which copyright exists, . [whether the personal computer 50 which the user of the personal computer accessed in quest of data distribution owns has just authentication data, and] Namely, a regular personal computer performs authenticating processing of whether to perform contents protection provided with sufficient security level, After enciphering music data (it is also called contents data below) with a predetermined cipher system to the personal computer which is performing just contents protection, The license as information required in order to reproduce such enciphered content data and enciphered content data is distributed to the personal computer 50.
[0101]In this case, the personal computer 50 can receive and manage enciphered content data and a license from the distributing server 10 with a different security level via the modem 40 and Internet network 30. That is, the personal computer 50 contains the license management device which realizes contents **** protection in hard, and the license management module which realizes contents protection in soft. A license management device obtains the help of application software, and receives enciphered content data and a license via Internet network 30 grade from the distributing server 10. This license management device establishes the encryption communication way for receiving the license for reproducing enciphered content data between distributing servers directly, and holds the received license in hard, and its security level is high. The encryption communication way according to a predetermined procedure is similarly established between distributing servers, and a license management module also records a license on a hard disk (it is called HDD), after receiving the license, enciphering and

protecting. Enciphered content data and a license are received and managed with a security level lower than a license management device.In the case of which, enciphered content data is recorded by HDD as it is. A license management device and a license management module are explained in detail later.
[0102]Henceforth, the security level which maintains confidentiality by hardwares, such as the memory card 110 or a license management device, in order to distinguish a security level and a license is called the level 2, Suppose that the license which requires the security of the level 2 and is transmitted from a distributing server is called level 2 license. Suppose that the license which similarly calls level 1 the security level which maintains confidentiality, requires the security level of level 1, and is transmitted from a distributing server by software like a license management module is called a level 1 license.
[0103]In drawing 1, the personal computer 50, The enciphered content data limited to the local use limited to personal use from the music data acquired from the audio CD (Compact Disk) 60 which recorded music data using the license management module, The license for reproducing enciphered content data is generable. This processing is called ripping and it is equivalent to the act which acquires enciphered content data and a license from an audio CD. On the character, since a security level is by no means high, even if ripping is made by what kind of means, it is treated as a level 1 license and the basis of the license of the local use by ripping is carried out. The details of ripping are mentioned later.
[0104]The personal computer 50, It is possible to transmit the enciphered content data and the license which were connected with the reproduction terminal 100 and received from the distributing server 10 with the USB (UniversalSerial Bus) cable 70 to the memory card 110 equipped by the reproduction terminal 100.
[0105]The personal computer 50 transmits the enciphered content data and the license which were received to the personal computer 80 via the telecommunication cable 90.
[0106]Therefore, in the data distribution system shown in drawing 1, The personal computer 50 acquires enciphered content data and a license from an audio CD while receiving enciphered content data and a license from the distributing server 10 via the modem 40 and Internet network 30. The memory card 110 with which the reproduction terminal 100 was equipped receives the enciphered content data and the license which the personal computer 50 acquired from the distributing server 10 or the audio CD 60. The user of the reproduction terminal 100 becomes possible [acquiring enciphered content data and a license from an audio CD] by passing the personal computer 50.
[0107]In drawing 1, it has the composition that a portable telephone user's reproduction terminal 100 is equipped with the removable memory card 110, for example. The memory card 110 receives the enciphered content data received with the reproduction terminal 100, and after it decodes the encryption performed in the above-mentioned distribution, it gives it to the music reproduction section (not shown) in the reproduction terminal 100.
[0108]furthermore -- a portable telephone user passes the head telephone 130 grade linked to the reproduction terminal 100, for example -- such contents data -- "-- reproducing, " carrying out and hearing is possible.
[0109]In drawing 1, the personal computer 50, It can restrict to the enciphered content data in which a license management module has the level 1 license managed directly using a license management module, and can have a function played using the music reproduction program which takes a license management module and close cooperation. Reproduction of enciphered content data with level 2 license will become possible if a personal computer is equipped with the contents playback circuit which has confidentiality by hardware with the same composition as a reproduction terminal. The

detailed explanation about the reproduction in a personal computer is omitted in order to simplify the explanation in this application.
[0110]If it is not the personal computer provided with a regular license management device or a license management module with the contents protection feature of security level sufficient by having such composition, Distribution of contents data is received from the distributing server 10, and it becomes difficult composition to transmit enciphered content data to the personal computer 80 or the reproduction terminal 100.
[0111]By and the thing for which the frequency is calculated in the distributing server 10 whenever it distributes the contents data for one music. If it supposes that the royalty generated whenever the user of a personal computer receives contents data (download) is collected with the usage fee of an Internet network, it will become easy for an owner of a copyright to secure a royalty.
[0112]In drawing 1, the reproduction terminal 100 assumes the reproduction terminal which does not have a function which carries out direct communication to the distributing server 10.
[0113]Being needed on a system, in order to make refreshable the contents data enciphered and distributed in composition as shown in drawing 1 at the user side of a personal computer, Are a method for distributing the encryption key in communication to the 1st, and to the further 2nd. It is the method itself which enciphers contents data to distribute, and is the composition of realizing contents data protection for preventing further the unapproved copy of the contents data distributed to the 3rd in this way.
[0114]In the time of distribution, movement, check-out, check-in, and generating of each reproductive session especially in an embodiment of the invention, The recorder and data reproduction terminal (the data reproduction terminal which can reproduce contents is also called the reproduction terminal or personal computer.) in which the attestation and the check function to the movement destination of these contents data were enriched, and un-attesting or a decode key was torn the following -- it is the same -- by preventing the output of the contents data to receive explains the composition which strengthens the copyright protection of contents data.
[0115]Suppose that the processing which transmits contents data to each personal computer is called "distribution" from the distributing server 10 in the following explanation.
[0116]In the data distribution system shown in drawing 1, drawing 2 is a figure explaining the characteristics, such as data for the communication used, and information.
[0117]First, the data distributed from the distributing server 10 is explained. Dc(s) are contents data of music data etc. Encryption which can decode the contents data Dc with the license key Kc is given. Enciphered content data {Dc} Kc to which encryption which can be decoded with the license key Kc was given is distributed to the user of a personal computer from the distributing server 10 in this form.
[0118]In the following, it shall be shown that the notation {Y} X gave encryption which can be decoded with the decode key X for the data Y.
[0119]From the distributing server 10, additional information Dc-inf as plaintext information, including the copyright about contents data or server access relation, is distributed with enciphered content data. Transaction ID which is the management codes for specifying distribution of the license key from license key Kc and the distributing server 10, etc. as a license is exchanged between the distributing server 10 and the personal computer 50. Transaction ID is used also in order to specify the license by distribution, i.e., the license of use on the local aiming at personal use. In order to distinguish what is depended on distribution, and the thing of local use, it is transaction ID of local use which starts in "0", and the head of transaction ID presupposes that it is a beginning [from other than "0"] thing transaction ID by distribution. The content ID

which is a code for identifying the contents data Dc as a license, . Are generated based on the license terms of purchase AC included the information, including the number of licenses, functional limitation, etc., determined by the specification from the user side. The reproduction control information ACp etc. which are the access control information ACm which is information about the restriction to access of the license in a recorder (a memory card or a license management device), and the control information in a data reproduction terminal exist. The access restriction information ACm is specifically the control information on the hand which suited the license or license key from a memory card, a license management module, and a license management module outside to the output, There are limitation information about movement and the duplicate of the number of times (number which outputs a license key for reproduction) of refreshable, and a license, a security level of a license, etc. In order to reproduce the reproduction control information ACp, after a contents playback circuit receives a license key, it is the information which restricts reproduction and a reproduction term, reproduction speed change restrictions, reproduction range specification (partial license), etc. occur.
[0120]Reproduction frequency <0 which is the control information to which the access restriction information ACm restricts reproduction frequency in an embodiment of the invention for simplification : Reproduction improper, Having the number of times of 1 - 254:refreshable, and no 255:restrictions, the move duplicate flag <0:move duplication prohibition and1 which restrict movement and the duplicate of a license :. Only movement can be 2:move reproduced [good and]. Security-level "1: Considering it as three items of level 1 and 2:level 2", the reproduction control information ACp shall restrict the reproduction term "UTCtime code" which is the control information which specifies a refreshable term. Therefore, henceforth, the reproduction control information ACp is also called the reproduction term ACp.
[0121]Suppose henceforth that transaction ID and content ID are combined, it is named license ID generically, the license key Kc, license ID, the access restriction information ACm, and the reproduction term ACp are combined, and it is named a license generically.
[0122]In an embodiment of the invention, for every class of the reproduction terminal which reproduces a recorder (a memory card, a license management device, and a license management module) and contents data. The prohibition class lists CRL (Class Revocation List) are employed so that distribution of contents data and reproduction can be forbidden. Below, the sign CRL may express the data in prohibition class lists if needed.
[0123]The reproduction terminal, memory card and license management module in which distribution of a license, movement, check-out, and reproduction are forbidden, and the prohibition class-lists data CRL which listed the class of the license management device are contained in prohibition class-lists pertinent information. All the apparatus and programs which are reproduced in response to the management and accumulation of a license, and the license in connection with contents data protection are the target of a listing.
[0124]While the prohibition class-lists data CRL is managed within the distributing server 10, record maintenance of it is carried out with a memory card and a license management module also into the hard disk (HDD) in the personal computer 50, or a license management device. Although it is necessary to upgrade such prohibition class lists at any time, and to update data, About change of data, when distributing the license of enciphered content data, a license key, etc. fundamentally, When the update date of the prohibition class lists received from the personal computer (a license management device or a license management module) is judged and it is judged that it is not updated, the updated prohibition class lists are distributed to a personal computer. Prohibition

class lists are the same as having been exchanged and having mentioned the data changing above also between a license management module, a license management device, and the reproduction terminal 100. About change of prohibition class lists, it is also possible to have composition which occurs from the distributing server 10 side and adds the difference data CRL only reflecting a changed part to the prohibition class lists CRL in a memory card, a hard disk, and a license management device according to this. About the update date CRLdate of prohibition class lists, it is recorded in the prohibition class lists CRL recorded in the memory card, the hard disk, and the license management device, and version management is performed by checking this by the distributing server 10 side. The difference data CRL update date CRLdate is contained.
[0125]The prohibition class lists CRL thus, by carrying out maintenance employment not only a distributing server but into a memory card or a personal computer, . A reproduction terminal and a memory card, or a decode key peculiar to the kind of personal computer (a license management device or a license management module) peculiar to a class namely, was torn. Supply of the license key to a reproduction terminal and a memory card, or a personal computer is forbidden. It becomes impossible for this reason, for reproduction of contents data to receive a license new in a memory card, a license management module, and a license management device in a reproduction terminal.
[0126]Thus, it is in a memory card or a license management device, or the prohibition class lists CRL in HDD which a license management module manages have composition which updates data one by one at the time of distribution. Management of the prohibition class lists CRL in a memory card, a license management module, and a license management device, Independently of an upper level, it records on a tamper resistant module (Tamper Resistant Module) with a memory card, a license management device, and the hard disk controlled by a license management module. Within a memory card or a license management device, It is recorded like a license with the Tampa resist module of the high level which guarantees confidentiality in hard, Alteration prevention treatment is performed at least and management of the prohibition class lists CRL recorded in HDD which a license management module manages is recorded on HDD of a personal computer, etc. by cipher processing. In other words, it is recorded by the tamper resistant joule of the low level the confidentiality was guaranteed to be by software. Anyway, it has composition which can alter the prohibition class-lists data CRL from an upper level with neither a file system nor an application program. As a result, copyright protection about data can be made firmer.
[0127]Drawing 3 is a figure explaining the characteristics, such as data for the attestation used in the data distribution system shown in drawing 1, and information.
[0128]The open encryption keys KPpy and KPmw peculiar to a reproduction terminal, a memory card, a license management device, and a license management module are formed, respectively, The open encryption keys KPpy and KPmw can be decoded, respectively with the secret decode key Kmw peculiar to the secret decode key Kpy and a memory card peculiar to a reproduction terminal, a license management device, and a license management module. These public presentation encryption key and a secret decode key have a different value for every kind of a reproduction terminal, a memory card, a license management device, and license management module. These open encryption keys and secret decode keys are named generically, a class key is called, and the unit which shares a class public presentation encryption key for these open encryption keys, and shares a class secret decode key and a class key for a secret decode key is called a class. A class changes with the kind of a manufacturing company or product, lots at the time of manufacture, etc.
[0129]Cpy is provided as a class certificate of a contents playback device (reproduction

terminal), and Cmw is provided as a memory card, a license management device, and a class certificate of a license management module.
[0130]These class certificates have different information for every class of a contents playback device, a memory card, a license management device, and a license management module. A tamper resistant module is torn, or to the class key with which the code with a class key was broken, namely, the class secret decode key was acquired, it is listed by prohibition class lists and is the prohibition target of transmission of a license.
[0131]A class public presentation encryption key and a class certificate peculiar to these contents playback devices, a memory card, a license management device, and a license management module, Authentication data {KPpy//Cpy} The form of KPa, or in the form of authentication data {KPmw//Cmw} KPa, it is recorded on a data reproduction device (reproduction terminal), a memory card, a license management device, and a license management module, respectively at the time of shipment. Although it will explain to details later, KPa is an open authentication key common to the whole distribution system.
[0132]As a key for managing data processing in the memory card 110, a license management device, and a license management module, The secret decode key Kmcx peculiar to each which can decode the data enciphered with the open encryption key KPmcx set up for every medium called a memory card, a license management device, and a license management module or software running and the open encryption key KPmcx exists. every memory card of this -- a child -- an another open encryption key and secret decode key are named generically, an individual key is called, the open encryption key KPmcx is called an individual public presentation encryption key, and the secret decode key Kmcx is called an individual secret decode key.
[0133]The data transfer between the outside of a memory card, and a memory card, or the data transfer between the outside of a license management device, and a license management device, Or as an encryption key for the maintenance of secret in the data transfer in a license management inter module, the outside of a license management module, Whenever distribution of contents data and reproduction are performed, the common keys Ks1-Ks3 generated in the distributing server 10, the reproduction terminal 100, the memory card 110, a license management device, and a license management module are used.
[0134]here, the common keys Ks1-Ks3 are a unit of communication of a distributing server, a reproduction terminal, a memory card, a license management device, or a license management inter module, or a unit of access -- "-- it being a peculiar common key by which it is generated in every session", and, Suppose that these common keys Ks1-Ks3 are also called a "session key" to below.
[0135]These session keys Ks1-Ks3 are managed by having a peculiar value for every session with a distributing server, a reproduction terminal, a memory card, a license management device, and a license management module. Specifically, session key Ks1 is generated for every distribution session by a distributing server. Session key Ks2 is generated for every distribution session and reproduction session with a memory card, a license management device, and a license management module, and session key Ks3 is generated for every reproduction session in a reproduction terminal. In each session, the security intensity in a session can be raised by delivering and receiving these session keys, and transmitting a license key etc. in response to the session key generated by other apparatus, after performing encryption by this session key.
[0136]A binding license required in order to relate with a license management device in order that drawing 4 may make movable the enciphered content data and the license which were acquired by software (license management module) to other personal

computers, and to encipher and manage, The checkout control information in the check-out session which lends out the enciphered content data and the license which were acquired by software to the memory card 110 is shown.
[0137]A level 1 license for a binding license to reproduce enciphered content data, The binding key which is a common key for enciphering the information about check-out of a license and realizing a soft tamper resistant module, ACmb and ACpb which are the control information over a binding license, Binding ID which is a general term for the transaction IDb which is transaction ID for a binding license, content ID b which is the straw men for binding ID, and the transaction IDb and content ID b is comprised. That is, since it is premised on what is recorded on a license management device as a license, it has the same composition as a license.
[0138]The binding key Kb manages the license of the enciphered content data acquired by software, and is held by hardware. And a license cannot be taken out if not based on the binding key Kb held by hardware. The control information ACmb and ACpb is equivalent to ACmACp contained in the license which reproduces enciphered content data, and has a fixed value. ACmb expresses the reproduction frequency restriction nothing of a license, move duplication prohibition, and the security level 1, and ACpb expresses that a reproduction term is indefinite.
[0139]Checkout control information comprises transaction ID with the number which can be checked out, and check-out place individual ID at the time of check-out. Whenever the number which can be checked out shows the number of times which can lend out enciphered content data and checks out enciphered content data, a numerical value is reduced every [1], and whenever he checks in at enciphered content data, a numerical value is increased by every [1]. Check-out place individual ID is identification information which specifies the memory card which checks out enciphered content data, and the individual public presentation encryption key KPmcx which a memory card holds corresponds. Transaction ID is transaction ID of local use used when you check out at the time of check-out.
[0140]Drawing 5 is a schematic block diagram showing the composition of the distributing server 10 shown in drawing 1. The distributing server 10 is provided with the following.
The data which enciphered contents data according to the prescribed method, and the information database 304 for holding delivery information, such as content ID.
The charge database 302 for holding the accounting information which followed the access start to contents data for every user of a personal computer.
The CRL database 306 which manages the prohibition class lists CRL.
The menu database 307 holding the menu of the contents data held at the information database 304, it is related with distribution of transaction ID which specifies distribution of contents data, a license key, etc. for every distribution of a license, [record and] The data from the distribution recording data base 308 to hold, the information database 304 and the charge database 302, the CRL database 306, the menu database 307, and the distribution recording data base 308 is received via bus BS1, The data processing part 310 for performing predetermined processing, and the communication apparatus 350 for performing data transfer between the distribution career 20 and the data processing part 310 via a communications network.

[0141]The data processing part 310 is provided with the following.
The distribution control part 315 for controlling operation of the data processing part 310 according to the data on bus BS1.
The session key generating part 316 for being controlled by the distribution control part 315 and generating session key Ks1 at the time of a distribution session.

The authentication key attaching part 313 holding the open authentication key KPa for decoding authentication data {KPmw//Cmw} KPa for the attestation sent from the license management device and the license management module.
Authentication data {KPmw//Cmw} KPa for the attestation sent from the license management device and the license management module is received via communication apparatus 350 and bus BS1, The decoding processing section 312 which performs decoding processing with the open authentication key KPa from the authentication key attaching part 313, Session key Ks1 generated from the session key generating part 316 is enciphered using the class public presentation encryption key KPmw obtained by the decoding processing section 312, The enciphering processing part 318 for outputting to bus BS1, and the decoding processing section 320 which performs decoding processing in response to the data transmitted after being enciphered by session key Ks1 from bus BS1.

[0142]The data processing part 310 is provided with the following.
The license key Kc and the access restriction information ACm which are given from the distribution control part 315, The enciphering processing part 326 for enciphering with the individual public presentation encryption key KPmcx of the memory card obtained by the decoding processing section 320, a license management device, and a license management module.
The enciphering processing part 328 for enciphering further and outputting the output of the enciphering processing part 326 to bus BS1 by session key Ks2 to which it is given from the decoding processing section 320.

[0143]The authentication key which a distributing server holds changes with security levels of the receiver which the license which a distributing server tends to distribute requires. If it is in the distributing server which distributes the level 2 license which requires the security level 2, authentication key KPa2 in which authenticating processing is possible is held to the authentication data which the apparatus of the level 2 transmits in a security level. If the distributing server which distributes the level 1 license which requires the security level 1 has the license which it is going to distribute, Also to any of the apparatus of level 1, since it can distribute, the apparatus and the security level of the level 2 will hold the level 2 and the authentication keys KPa2 and KPa1 corresponding to each of level 1, and a security level will use properly according to a partner's level. The authentication key which the transmitted authentication data needs, Even if enciphered as authentication data of the class certificate Cmw, in addition, it is indicated to the field maintained as a plaintext, and the distribution control part 315 of the distributing server 10 has the composition that an authentication key can be easily specified before decoding by the decoding processing section 312. In order to distinguish two authentication keys, authentication key KPa1 corresponding to level 2 authentication key KPa2 and level 1 for authentication key KPa2 corresponding to the level 2 is called level 1 authentication key KPa1, and it is generally called the authentication key KPa.
[0144]The operation in the distribution session of the distributing server 10 will be later explained in detail using a flow chart.
[0145]Drawing 6 is a schematic block diagram for explaining the composition of the personal computer 50 shown in drawing 1. The personal computer 50 is provided with the following.
Bus BS2 for performing data transfer of each part of the personal computer 50.
The controller (CPU) 510 for controlling the inside of a personal computer and executing various kinds of programs.

Data bus BS2.
The hard disk (HDD) 530 and CD-ROM drive 540 which are the mass recorders for being connected to data bus BS2, recording a program and data, and accumulating, The keyboard 560 for inputting the directions from a user, and the display 570 for giving a user various kinds of information visually.

[0146]The personal computer 50 is provided with the following.
USB interface 550 for controlling transfer of data between the controller 510 and the terminal 580, when communicating enciphered content data and a license in reproduction terminal 100 grade.
The terminal 580 for connecting USB cable 70.
Serial interface 555 for controlling transfer of data between the controller 510 and the terminal 585, when communicating via the distributing server 10, Internet network 30, and the modem 40.
The terminal 585 for connecting with the modem 40 with a cable.

[0147]The controller 510 is executing an application program, In order to receive enciphered content data etc. from the distributing server 10 to the license management device 520 or the license management module 511 via Internet network 30, While controlling transfer of data between the distributing servers 10, control at the time of acquiring enciphered content data and a license from an audio CD by ripping via CD-ROM drive 540 is performed.
[0148]The personal computer 50 is provided with the following.
The license management device 520 which manages the license for exchanging various kinds of keys between the distributing servers 10 when performing reception of the enciphered content data from the distributing server 10, and a license, and reproducing the distributed enciphered content data in hard.
The contents managing module 511 which generates the exclusive license which is a program executed by the controller 510, performed reception of the enciphered content data from the distributing server 10, and a level 1 license by a program, and gave encryption original with the received license.

[0149]Since it is what the license management device 520 delivers and receives the data at the time of receiving enciphered content data and a license from the distributing server 10, and manages in hard the license received in hard, It comes out to treat the license of the level 2 which requires a high security level. On the other hand, the license management module 511 performs transfer of the data at the time of receiving enciphered content data and a license from the distributing server 10 in soft using the program executed with a moveable cooking stove and the roller 510, Ripping performs the enciphered content data of local use, and generation of a license for reception of a license from an audio CD again, Cipher processing etc. are performed and protected against the acquired license, and since it is what is accumulated in HDD530 and managed, only the level 1 license whose security level is lower than the license management device 520 is treated. When a high security level is the level 2, it cannot be overemphasized that a level 1 license can also be treated.
[0150]Thus, the personal computer 50, The license management module 511 and the license management device 520 for receiving enciphered content data and a license via Internet network 30 from the distributing server 10, CD-ROM drive 540 for acquiring enciphered content data and a license from an audio CD by ripping is built in.
[0151]Drawing 7 is a schematic block diagram for explaining the composition of the reproduction terminal 100 shown in drawing 1.

[0152]The reproduction terminal 100 is provided with the following.
Bus BS3 for performing data transfer of each part of the reproduction terminal 100.
The controller 1106 for controlling operation of the reproduction terminal 100 via bus BS3.
The navigational panel 1108 for giving the directions from the outside to the reproduction terminal 100.
The display panel 1110 for giving a portable telephone user the information outputted from controller 1106 grade as vision information.

[0153]The reproduction terminal 100 is provided with the following.
The removable memory card 110 for memorizing and carrying out decoding processing of the contents data (music data) from the distributing server 10.
The memory interface 1200 for controlling transfer of the data between the memory card 110 and bus BS3.
USB interface 1112 for controlling the data transfer between bus BS3 and the terminal 1114, when receiving enciphered content data and a license from the personal computer 50.
The terminal 1114 for connecting USB cable 70.

[0154]. The reproduction terminal 100 is further set to every [of a reproduction terminal] kind (class), respectively. The authentication data attaching part 1500 holding authentication data {KPp1//Cp1} KPa2 enciphered in the state where the justification can be attested by decoding class public presentation encryption key KPp1 and class certificate Cp1 with the class public presentation authentication key KPa is included. Here, the class y of the reproduction terminal 100 presupposes that it is y= 1. Since a reproduction terminal is apparatus which provides reproduction using the contents playback device which can hold confidentiality in hard, a security level is the level 2.
[0155]The reproduction terminal 100 is provided with the following.
The Kp1 attaching part 1502 holding Kp1 which is a class secret decode key of a reproduction terminal (contents playback device).
The decoding processing section 1504 which obtains session key Ks2 which decoded the data which received from bus BS3 by Kp1, and was generated by the memory card 110.

[0156]The reproduction terminal 100 is provided with the following.
The session key generating part 1508 which generates session key Ks3 for enciphering the data which sets and is carried out on bus BS3 between the memory cards 110 in the reproduction session which reproduces the contents data memorized by the memory card 110 with a random number etc.
When receiving the license key Kc and the reproduction term ACp from the memory card 110 in the reproduction session of enciphered content data, The enciphering processing part 1506 which enciphers session key Ks3 generated by the session key generating part 1508 by session key Ks2 obtained by the decoding processing section 1504, and is outputted to bus BS3.

[0157]The reproduction terminal 100 is provided with the following.
The decoding processing section 1510 which decodes the data on bus BS3 by session key Ks3, and outputs the license key Kc and the reproduction term ACp.
The decoding processing section 1516 which decodes in response to enciphered content data {Dc} Kc with the license key Kc acquired from the decoding processing section 1510, and outputs contents data from bus BS3.

The music reproduction section 1518 for reproducing contents data in response to the output of the decoding processing section 1516.
The terminal 1530 for outputting the output of DA converter 1519 which changes the output of the music reproduction section 1518 into an analog signal from a digital signal, and DA converter 1519 to external output devices (graphic display abbreviation), such as a head telephone.

[0158]In drawing 7, the field enclosed with a dotted line constitutes the contents playback device 1550 which decodes enciphered content data and reproduces music data. In drawing 7, for the simplification of explanation, only the block in connection with reproduction of the music data of this invention is indicated among reproduction terminals, and the statement is omitted in part about the block about the talking function with which the reproduction terminal is originally provided.
[0159]The operation in each session of each component part of the reproduction terminal 100 will be later explained in detail using a flow chart.
[0160]Drawing 8 is a schematic block diagram for explaining the composition of the memory card 110. As already explained, as an open encryption key peculiar to a memory card, and a secret decode key, KPmw and Kmw are provided and the class certificate Cmw of a memory card is formed, but. In the memory card 110, it shall be expressed with the natural number x= 4 which is the natural number w= 3 which identifies the class of a memory card, and identifies a memory card, respectively. Since the memory card 110 is apparatus which holds confidentiality in hard, a security level is 2.
[0161]Therefore, the memory card 110 is provided with the following.
The authentication data attaching part 1400 holding authentication data {KPm3//Cm3} KPa2.
The Kmc attaching part 1402 holding individual secret decode key Kmc4 which is a peculiar decode key set up for every memory card.
The Km attaching part 1421 holding peculiar class secret decode key Km3 set up for every kind of memory card.
The KPmc attaching part 1416 holding open encryption key KPmc4 which can be decoded by individual secret decode key Kmc4.

[0162]Thus, by forming the encryption key of a recorder called a memory card, it becomes possible to perform management of the distributed contents data or the enciphered license key per memory card so that it may become clear in the following explanation.
[0163]The memory card 110 is provided with the following.
The interface 1424 which delivers and receives a signal via the terminal 1426 between the memory interfaces 1200.
Bus BS4 which exchanges a signal between the interfaces 1424.
The decoding processing section 1422 which outputs session key Ks1 which the distributing server 10 generated in the distribution session from the Km attaching part 1421 for every kind of memory card in response to the fact that peculiar class secret decode key Km3 to contact Pa from the data given to bus BS4 from the interface 1424. Perform decoding processing by level 2 authentication-key KPa2 from the data given to bus BS4 from the KPa attaching part 1414 in response to the fact that level 2 authentication-key KPa2, and a decoding result and the obtained class certificate for the controller 1420. The decoding processing section 1408 which outputs the obtained class public key to the enciphering processing part 1410, and the enciphering processing part 1406 which enciphers the data selectively given by the change-over switch 1446, and is

outputted to bus BS4 with the key selectively given by the change-over switch 1442.

[0164]The memory card 110 is provided with the following.
The session key generating part 1418 which generates session key Ks2 in each session.
The enciphering processing part 1410 which enciphers session key Ks2 which the session key generating part 1418 outputted with the class public presentation encryption keys KPpy and KPmw obtained by the decoding processing section 1408, and is sent out to bus BS4.
The decoding processing section 1412 decoded by session key Ks2 obtained from the session key generating part 1418 in response to the data enciphered by session key Ks2 from bus BS4.
The cipher-processing part 1417 which enciphers the license key Kc and the reproduction term ACp which were read from the memory 1415 in the reproduction session of enciphered content data with the individual public presentation encryption key KPmcx peculiar to other memory cards 110 decoded by the decoding processing section 1412 (!=4).

[0165]The decoding processing section 1404 for the memory card 110 to decode the data on bus BS4 further by individual public presentation encryption key KPmc4 and individual secret decode key Kmc4 [peculiar to the memory card 110] which make a pair, The prohibition class-lists data CRL and enciphered content data {Dc} Kc, Enciphered content data {Dc} The license (Kc, ACp, ACm, license ID) for reproducing Kc, The memory 1415 for storing in response to additional information Data-inf, the reproduction list file of enciphered content data, and the license management file for managing a license from bus BS4 is included. The memory 1415 is constituted by semiconductor memory, for example. The CRL field 1415A for the memory 1515 to record the prohibition class lists CRL, The license area 1415B which records a license, and enciphered content data {Dc} Kc, The reproduction list file which records the fundamental information for accessing enciphered content data and the license which were recorded on pertinent information Dc-inf of enciphered content data, and a memory card, And the data area 1415C in which the exterior which records the license management file which records information required in order to manage a license for every enciphered content data to direct access is possible is comprised. The details of a license management file and a reproduction list file are mentioned later.
[0166]The license area 1415B stores a license per record only for a license called an entry, in order to record a license (contents key Kc, the reproduction control information ACp, access-restriction-information ACm, license ID). In accessing to a license, the license has the composition of it being stored or specifying an entry to record a license on with an entry number.
[0167]Further, the memory card 110 performs data transfer between the exteriors via bus BS4, and contains the controller 1420 for controlling operation of the memory card 110 in response to reproduction information etc. between bus BS4.
[0168]All the composition except the data area 1415C is constituted by the Tampa-proof module field.
[0169]Drawing 9 is a schematic block diagram showing the composition of the license management device 520 built in the personal computer 50. The point that the license management device 520 does not need the field equivalent to the data area 1415C in MEMOKADO 110, Only by differing in that it has the interface 5224 and the terminal 5226 which differ in the function of the interface 1424, and the shape of the terminal 1426, the same composition as the memory card 110 is comprised fundamentally. The authentication data attaching part 5200 of the license management device 520, the Kmc

attaching part 5202, the decoding processing section 5204, the cipher-processing part 5206, the decoding processing section 5208, the cipher-processing part 5210, the decoding processing section 5212, the KPa attaching part 5214, the KPmc attaching part 5216, The cipher-processing part 5217, the session key generating part 5218, the controller 5220, the Km attaching part 5221, the decoding processing section 5222, the interface 5224, the terminal 5226, and the change-over switch 5242-5246, Respectively, The authentication data attaching part 1400 of the memory card 110, the Kmc attaching part 1402, the decoding processing section 1404, the cipher-processing part 1406, the decoding processing section 1408, the cipher-processing part 1410, the decoding processing section 1412, the KPa attaching part 1414, the KPmc attaching part 1416, the cipher-processing part 1417, It is the same as the session key generating part 1418, the controller 1420, the Km attaching part 1421, the decoding processing section 1422, and the change-over switch 1442-1446. However, the authentication data attaching part 5200 holds authentication data {KPm7//Cm7} KPa2, and the KPmc attaching part 5216, Individual public presentation encryption key KPm8 is held, the Km attaching part 5202 holds class secret decode key Km7, and the Kmc attaching part 5221 holds individual secret decode key Kmc8. The natural number w showing the class of the license management device 520 is w= 7, and the natural number x for identifying the license management device 520 presupposes that it is it x= 8.

[0170]The memory 5215 which records the prohibition class lists CRL and a license (Kc, ACp, ACm, license ID) is replaced with the memory 1415 of the memory card 110, and the license management device 520 contains it. The memory 5215 comprises the CRL field 5215A which recorded the prohibition class lists CRL, and the license area 5215B which recorded the license.

[0171]The license management device 520 needs to hold the binding license which the license management module 511 uses. Therefore, the KPa attaching part 5214 holds the two authentication keys KPa2 and KPa1. The control from a different level will be later explained in detail using a flow chart.

[0172]The license management module 511 is a program which manages a license, and a security level is 1. The natural number w which expresses the class of the license management module 511 since the license management module 511 is a control program with the almost same composition as the license management device 520 is w= 5, The natural number x for identifying the license management device 520 presupposes that it is x= 6. Therefore, the license management module 511 holds authentication data {KPm5//Cm5} KPa1, individual public presentation encryption key KPm6, class secret decode key Km5, and individual secret decode key Kmc6. The two authentication keys KPa2 and KPa1 are held.

[0173]Hereafter, operation of each session in the data distribution system shown in drawing 1 is explained.

[0174][Initialization] Initialization performed before the personal computer 50 receives distribution of enciphered content data and a license from the distributing server 10 is explained.

[0175]Drawing 10 - drawing 12 are the 1st for explaining initialization performed before the personal computer 50 receives enciphered content data and a license from the distributing server 10 - the 3rd flow chart.

[0176]When generation of a biding license is requested via the keyboard 560 with reference to drawing 10 (Step S10), the license management module 511, The binding key Kb is generated (Step S12), it ranks second and the transaction IDb, content ID b, and the predetermined control information ACmb and ACpb are generated (Step S14). Step S12 and S14 are the generation processings of a binding license.

[0177]And the license management module 511 directs the output of authentication data

via bus BS2 to the license management device 520 (Step S16).
[0178]So then, the controller 5220 of the license management device 520, The output instruction of authentication data is received via the terminal 5226, the interface 5224, and bus BS5, Authentication data {KPm7//Cm7} KPa2 is acquired from the authentication data attaching part 5200 via bus BS5, and authentication data {KPm7//Cm7} KPa2 is outputted via bus BS5, the interface 5224, and the terminal 5226 (Step S18). The license management module 511 receives authentication data {KPm7//Cm7} KPa2 via bus BS2 (Step S20), and decodes authentication data {KPm7//Cm7} KPa by level 2 authentication-key KPa2 (Step S22).
[0179]The license management module 511 from a decoding processing result. [whether processing was performed normally and] Namely, in order that the license management device 520 may attest holding open encryption key KPm7 and certificate Cm7 from a regular license pipe device, Authenticating processing which judges whether the authentication data which gave the code for proving the justification in a regular organization was received is performed (Step S24). When it is judged that it is just authentication data, the license management module 511 recognizes and receives open encryption key KPm7 and certificate Cm7. And it shifts to the next processing (Step S26). In not being just authentication data, it is considered as non approval, and it ends processing without receiving open encryption key KPm7 and certificate Cm7 (Step S68).
[0180]When it is recognized as a result of attestation that it is regular apparatus, the license management module 511, Next, it refers for whether class certificate Cm7 of the license management device is listed by the prohibition class lists CRL to the hard disk (HDD) 530, When these class certificates have been the targets of prohibition class lists, initialization is completed here (Step S68).
[0181]On the other hand, when the class certificate of the license management device 520 is outside the object of prohibition class lists, it shifts to the next processing (Step S26).
[0182]If it is checked as a result of attestation that it is access from a license management device with just authentication data, and a class is outside the object of prohibition class lists, the license management module 511 will generate session key Ks2a (Step S28).
[0183]With reference to drawing 11, the license management module 511, Session key Ks2a is enciphered by class public presentation encryption key KPm7, encryption data [Ks2] {a} Km7 is generated (Step S30), and encryption data [Ks2] {a} Km7 is outputted to the license management device 520 via bus BS2 (Step S32). The controller 5220 of the license management device 520, Receive encryption data [Ks2] {a} Km7 via the terminal 5226, the interface 5224, and bus BS5, and the decoding processing section 5222, By class secret decode key Km7 outputted from the Km attaching part 5221, encryption data [Ks2] {a} Km7 is decoded and session key Ks2a is received (Step S34). In connection with having received session key Ks2a, the controller 5220 controls the session key generating part 5218, and generates session key Ks2b. So then, the session key generating part 5218, Generate session key Ks2b (Step S36), and the controller 5220, The update date CRLdate of the prohibition class lists CRL is acquired from the CRL field 5215A of the memory 5215 via bus BS5, and the acquired update date CRLdate is outputted to the change-over switch 5246 via bus BS5 (Step S38). ******** and the cipher-processing part 5206 encipher session key Ks2b and individual public presentation encryption key KPmc8 and the update date CRLdate which were received by switching the change-over switch 5246 one by one by session key Ks2a from the decoding processing section 5222. The controller 5220 outputs Ks2b//KPmc8//encryption data {CRLdate} Ks2a on bus BS5 via the interface 5224 and

the terminal 5226 (Step S40).
[0184]The license management module 511 receives Ks2b//KPmc8//encryption data {CRLdate} Ks2a via bus BS2, Ks2b//KPmc8//encryption data {CRLdate} Ks2a is decoded by session key Ks2a, and session key Ks2b, individual public presentation encryption key KPmc8, and the update date CRLdate are received (Step S42). And the license management module 511, Step S12, the binding license generated by S14 (it transaction-IDb(s) and) Content ID b, the binding key Kb, and the control information ACmb and ACpb are enciphered by open encryption key KPmc8, and encryption data {transaction IDb// content ID b//Kb//ACmb//ACpb} Kmc8 is generated (Step S44).
[0185]With reference to drawing 12, the update date CRLdate of the prohibition class lists transmitted from the license management device 520 in the license management module 511 from the update date of the prohibition class lists CRL currently held at the hard disk (HDD) 530, It is compared whether the prohibition class lists which any hold are new. When the prohibition class lists CRL of the license management device 520 are newer, it shifts to Step S48. Conversely, when the prohibition class lists CRL of the license management module 511 are newer, it shifts to Step S52 (Step S46).
[0186]When the direction of the prohibition class lists CRL of the license management device 520 is judged to be new, the license management module 511, Encryption data {transaction IDb// content ID b//Kb//ACmb//ACpb} Kmc8 is enciphered with session key Ks2b generated in the license management device 520, Encryption data {{transaction IDb// content ID b//Kb//ACmb//ACpb} Kmc8} Ks2b is outputted to the license management device 520 via bus BS2 (Step S48).
[0187]And the controller 5220 of the license management device 520, Encryption data {{transaction IDb// content ID b//Kb//ACmb//ACpb} Kmc8} Ks2b is received via the terminal 5226 and the interface 5224, It decodes with session key Ks2b generated by the session key generating part 5218, and {transaction IDb// content ID b//Kc//ACmb//ACpb} Kmc8 is received (Step S50). Then, it shifts to Step S60.
[0188]When the direction of the prohibition class lists CRL of the license management module 511 is judged to be new, on the other hand in the license management module 511, the license management module 511, In order to update the prohibition class lists CRL which the license management device 520 holds, an updated part after the update date CRLdate is acquired from HDD530 as the difference CRL via bus BS2 (Step S52).
[0189]And the license management module 511, The difference CRL of prohibition class lists, and encryption data {transaction IDb// content ID b//Kb//ACmb//ACpb} Kmc8, It enciphers with session key Ks2b generated in the license management device 520, Encryption data {CRLdate//{transaction IDb// content ID b//Kb//ACmb//ACpb} Kmc8} Ks2b is outputted to the license management device 520 via bus BS2 (Step S54).
[0190]The controller 5220 of the license management device 520 decodes the received data given to bus BS5 by the decoding processing section 5212 via the terminal 5226 and the interface 5224. The decoding processing section 5212 decodes the received data of bus BS5 using session key Ks2b given from the session key generating part 5218, and outputs them to bus BS5 (Step S56).
[0191]In this stage, {transaction IDb// content ID b//Kb//ACmb//ACpb} Kmc8 which can be decoded by individual secret decode key Kmc8 held at the Kmc attaching part 5221, and the difference CRL are outputted to bus BS5 (Step S56). The CRL field 5215A in the memory 5215 is updated based on the difference CRL by the difference CRL received with directions of the controller 5220 (Step S58).
[0192]Step S48 and S50 from the prohibition class lists CRL of the license management module 511 of the transmitting side. It is a send action to the license management devices 520, such as the binding key Kb when the prohibition class lists CRL of the license management device 520 of a receiver are new, Step S52, S54, S56, and S58, It is

a send action to the license management devices 520, such as the binding key Kb when the prohibition class lists CRL of the license management module 511 of the transmitting side are newer than the prohibition class lists CRL of the license management device 520 of a receiver. Thus, when the update date CRLdate of the prohibition class lists sent from the license management device 520 is compared and the prohibition class lists CRL of a receiver are older than the prohibition class lists CRL of the transmitting side, He is trying to make the always new prohibition class lists CRL hold by acquiring the difference CRL which is difference data of prohibition class lists from HDD530, and distributing the difference CRL to the license management device 520.

[0193]With directions of the controller 5220 after Step S50 or Step S58. Encryption data {transaction IDb// content ID b//Kb//ACmb//ACpb} Kmc8, In the decoding processing section 5204, it is decoded by secret decode key Kmc8 and a binding license (the binding key Kb, the transaction IDb, content ID b, control information ACmZ and ACp) is received (Step S60).

[0194]And the license management module 511, The entry number "0" for storing a binding license is inputted into the license management device 520 (Step S62), The controller 5220 of the license management device 520, The entry number "0" is received via the terminal 5226, the interface 5224, and bus BS5, A biding license (the transaction IDb, content ID b, the binding key Kb, the control information ACmb and ACpb) is stored in the field specified with the entry number "0" received among the license areas 5215B of the memory 5215 (Step S64).

[0195]In order that the license management module 511 may record the binding key Kb, the field of the license management device 520 is checked, A series of processings to Step 42 of drawing 11 from Step 16 of drawing 10 which prepares registration "Device confirming processing", A series of processings from Step S44 of drawing 11 which stores the binding key Kb in the license area 5215B of the license management device 520 to Step S64 of drawing 12 are called "binding key registration processing."

[0196]On the other hand, the license management module 511 generates the confidential file of a plaintext **** in extra sensitive information (a level 1 license and check-out information), With the binding key Kb, the encryption confidential file 160 which enciphered the confidential file is generated, the encryption confidential file 160 is recorded on HDD530 (Step S66), and operation of initialization is ended (Step S68).

[0197]Thus, the license management module 511 of the personal computer 50, The inside of the license area 5215B of the memory [in / a binding license is generated in initializing operation and / the license management device 520] 5215, While storing the binding license generated to the field specified with an entry number "0", the encryption confidential file 160 which enciphered the confidential file with the binding key Kb contained in the generated binding license is generated. And this encryption confidential file 160 is because the license received from the distributing server 10 with the license management module 511 is stored. Since a license cannot be taken out from the encryption confidential file 160 if there is no binding key Kb by enciphering a confidential file with the binding key Kb in this way, The binding key Kb is a common key for managing the license of enciphered content data. And since this binding key Kb is stored in the memory 5215 of the license management device 520, it can manage the binding key Kb by hardware. As a result, the license of the enciphered content data managed in soft by the encryption confidential file 160 recorded on HDD530 via the binding key Kb will be managed by hardware. Therefore, the enciphered content data and the license which were received by software are movable to other personal computers 80 so that it may mention later.

[0198][Distribution 1] Next, in the data distribution system shown in drawing 1, the

operation which distributes the level 2 license which requires enciphered content data and the security level 2 of the license management device 520 of the personal computer 50 from the distributing server 10 is explained. This operation is called "distribution 1."
[0199]The distribution operation to the license management device 520 built in the personal computer 50 which generates drawing 13 - drawing 16 at the time of the purchase of the enciphered content data in the data distribution system shown in drawing 1. They are the 1st for explaining (it is also hereafter called a distribution session) - the 4th flow chart.
[0200]Before the processing in drawing 13, the user of the personal computer 50 connects via the modem 40 to the distributing server 10, and is premised on acquiring the content ID to the contents which wish to purchase.
[0201]With reference to drawing 13, the distribution request by specification of content ID is made via the keyboard 560 from the user of the personal computer 50 (Step S100). And the terms of purchase AC for purchasing the license of enciphered content data via the keyboard 560 are inputted (Step S102). That is, in order to purchase the license key Kc which decodes selected enciphered content data, the access restriction information ACm and the reproduction term ACp of enciphered content data are set up, and the terms of purchase AC are inputted.
[0202]If the terms of purchase AC of enciphered content data are inputted, the controller 510 will give the output instruction of authentication data to the license management device 520 via bus BS2 (Step S104). The controller 5220 of the license management device 520 receives the output instruction of authentication data via the terminal 5226, the interface 5224, and bus BS5. And the controller 5220 reads authentication data {KPm7//Cm7} KPa2 from the authentication data attaching part 5200 via bus BS5, {KPm7//Cm7} KPa2 is outputted via bus BS5, the interface 5224, and the terminal 5226 (Step S106).
[0203]The controller 510 of the personal computer 50, In addition to authentication data {KPm7//Cm7} KPa2 from the license management device 520, the data AC and the distribution request of content ID and license terms of purchase are transmitted to the distributing server 10 (Step S108).
[0204]In the distributing server 10, from the personal computer 50 to a distribution request. The data AC of content ID, authentication data {KPm7//Cm7} KPa2, and license terms of purchase is received (Step S110), Decoding processing is performed for the authentication data outputted from the license management device 520 in the decoding processing section 312 with the level 2 authentication key KPa (Step S112).
[0205]Authenticating processing which judges whether the distribution control part 315 received the authentication data which gave the code for proving the justification in a regular organization from the decoding processing result in the decoding processing section 312 is performed (Step S114). When it is judged that it is just authentication data, the distribution control part 315 recognizes and receives class public presentation encryption key KPm7 and class certificate Cm7. And it shifts to the next processing (Step S116). In not being just authentication data, it is considered as non approval, and it ends a distribution session without receiving class public presentation encryption key KPm7 and class certificate Cm7 (Step S198). Temporarily, by level 2 authentication key KPa2, supposing it is performing the distribution request from level 1, since the authentication data of level 1 cannot be attested, processing will be ended here.
[0206]When it is regular authentication data and class public presentation encryption key KPm7 and class certificate Cm7 are recognized as a result of attestation, the distribution control part 315, Next, it refers for whether class certificate Cm7 of the license management device is listed by the prohibition class lists CRL to the CRL database 306, When these class certificates have been the targets of prohibition class

lists, a distribution session is ended here (Step S198).
[0207]On the other hand, when the class certificate of the license management device 520 is outside the object of prohibition class lists, it shifts to the next processing (Step S116).
[0208]In [if it is checked that it is access from the personal computer provided with a license management device with just authentication data as a result of attestation, and a class is outside the object of prohibition class lists] the distributing server 10, The distribution control part 315 generates transaction ID which is the management codes for specifying distribution (Step S118). The session key generating part 316 generates session key Ks1 for distribution (Step S120). Session key Ks1 is enciphered by the enciphering processing part 318 by class public presentation encryption key KPm7 corresponding to the license management device 520 obtained by the decoding processing section 312 (Step S122).
[0209]Transaction ID and session key Ks1 which were enciphered are outputted outside via bus BS1 and the communication apparatus 350 as transaction ID//{Ks1} Km7 (Step S124).
[0210]If the personal computer 50 receives transaction ID//{Ks1} Km7 with reference to drawing 14 (Step S126), the controller 510 will input transaction ID//{Ks1} Km7 into the license management device 520 (Step S128). In [if it does so] the license management device 520, The received data given to bus BS5 via the terminal 5226 and the interface 5224, By carrying out decoding processing to the license management device 520 held at the attaching part 5221 by class secret decode key Km7, the decoding processing section 5222 decodes session key Ks1, and receives session key Ks1 (Step S130).
[0211]The controller 5220 directs generation of session key Ks2 generated in the license management device 520 to the session key generating part 5218 at the time of distribution operation, if acceptance of session key Ks1 generated with the distributing server 10 is checked. And the session key generating part 5218 generates session key Ks2 (Step S132).
[0212]In a distribution session, the controller 5220 extracts the prohibition class lists CRL currently recorded on the memory 5215 in the license management device 520 to the update date CRLdate from the memory 1415, and outputs it to the change-over switch 5246 (Step S134).
[0213]The enciphering processing part 5206 by session key Ks1 given from the decoding processing section 5222 via contact Pa of the change-over switch 5242. The update date CRLdate of session key Ks2 given by switching the point of contact of the change-over switch 5246 one by one, individual public presentation encryption key KPmc8, and prohibition class lists is enciphered as one data row, {Ks2//KPmc8//CRLdate} Ks1 is outputted to bus BS3 (Step S136).
[0214]Ks2//KPmc8//encryption data {CRLdate} Ks1 outputted to bus BS3, It is outputted to the personal computer 50 via the interface 5224 and the terminal 5226 from bus BS3, and is transmitted to the distributing server 10 from the personal computer 50 (Step S138).
[0215]The distributing server 10 receives transaction ID//{Ks2//KPmc8//CRLdate} Ks1, In the decoding processing section 320, decoding processing by session key Ks1 is performed, The update date CRLdate of the prohibition class lists in session key Ks2 generated with the license management device 520, individual public presentation encryption key KPmc8 [peculiar to the license management device 520], and the license management device 520 is received (Step S142).
[0216]The distribution control part 315 generates the access restriction information ACm and the reproduction term ACp according to the content ID and the license terms

of purchase AC which were acquired at Step S110 (Step S144). The license key Kc for decoding enciphered content data is acquired from the information database 304 (Step S146).

[0217]The distribution control part 315 gives the generated license, i.e., transaction ID, content ID, license key Kc, the reproduction term ACp, and the access restriction information ACm to the enciphering processing part 326. The enciphering processing part 326, By individual public presentation encryption key KPmc8 [peculiar to the license management device 520] obtained by the decoding processing section 320, a license is enciphered and encryption data {transaction ID// content ID//Kc//ACm//ACp} Kmc8 is generated (Step S148).

[0218]With reference to drawing 15, the update date CRLdate of the prohibition class lists transmitted from the license management device 520 in the distributing server 10. When it is judged by comparing with the update date of the prohibition class lists CRL of the distributing server 10 held at the CRL database 306 whether the prohibition class lists CRL to hold are the newest in the license management device 520 and it is judged as the newest, it shifts to Step S152. When it is not the newest, it shifts to Step S160 (Step S150).

[0219]When judged as the newest, the enciphering processing part 328, Encryption data {transaction ID// content ID//Kc//ACm//ACp} Kmc8 outputted from the enciphering processing part 326 is enciphered by session key Ks2 generated in the license management device 520, Encryption data {{transaction ID// content ID//Kc//ACm//ACp} Kmc8} Ks2 is outputted to bus BS1. And the distribution control part 315 transmits encryption data {{transaction ID// content ID//Kc//ACm//ACp} Kmc8} Ks2 on bus BS1 to the personal computer 50 via the communication apparatus 350 (Step S152).

[0220]And the controller 510 of the personal computer 50 receives encryption data {{transaction ID// content ID//Kc//ACm//ACp} Kmc8} Ks2 (Step S154), and inputs it into the license management device 520 via bus BS5. The decoding processing section 5212 of the license management device 520, Encryption data {{transaction ID// content ID//Kc//ACm//ACp} Kmc8} Ks2 is received via the terminal 5226 and the interface 5224, It decodes by session key Ks2 generated by the session key generating part 5218, and {transaction ID// content ID//Kc//ACm//ACp} Kmc8 is received (Step S158). Then, it shifts to Step S172.

[0221]On the other hand, if it is judged that it is not the newest, the distribution control part 315 will acquire the newest prohibition class lists CRL from the CRL database 306 via bus BS1, and will generate the difference CRL which is difference data (Step S160).

[0222]The enciphering processing part 328 is enciphered by session key Ks2 generated in the license management device 520 in response to the output of the enciphering processing part 326, and the difference CRL of the prohibition class lists which the distribution control part 315 supplies via bus BS1. Difference CRL/encryption data {/{transaction ID// content ID//Kc//ACm//ACp} Kmc8} Ks2 outputted from the enciphering processing part 328 is transmitted to the personal computer 50 via bus BS1 and the communication apparatus 350 (Step S162).

[0223]The personal computer 50 receives difference CRL/encryption data {/{transaction ID// content ID//Kc//ACm//ACp} Kmc8} Ks2 transmitted (Step S164), It inputs into the license management device 520 via bus BS5 (Step S166). In the license management device 520, the received data given to bus BS5 are decoded by the decoding processing section 5212 via the terminal 5226 and the interface 5224. The decoding processing section 5212 decodes the received data of bus BS5 using session key Ks2 given from the session key generating part 5218, and outputs them to bus BS5 (Step S168).

[0224]In this stage, encryption license {transaction ID// content ID//Kc//ACm//ACp} Kmc8} which can be decoded by secret decode key Kmc8 held at the Kmc attaching part 5221, and the difference CRL are outputted to bus BS5 (Step S168). The CRL field 5215A in the memory 5215 is updated based on the difference CRL by the difference CRL received with directions of the controller 5220 (Step S170).
[0225]Step S152, S154, S156, and S158, It is distribution operation to the license management devices 520, such as the license key Kc in case the prohibition class lists CRL which the license management device 520 holds are the newest, Step S160, S162, S164, S166, S168, and S170 are distribution operations to the license management devices 520, such as the license key Kc in case the prohibition class lists CRL which the license management device 520 holds are not the newest. Thus, when the update date CRLdate of the prohibition class lists sent from the license management device 520 checks in detail whether it is the newest update date and is not the newest, The outflow of the distributed license to the license management device with which the license was broken can be prevented by acquiring the newest prohibition class lists CRLdate from the CRL database 306, and distributing the difference CRL to the license management device 520.
[0226]With directions of the controller 5220 after Step S158 or Step S170. Encryption license {transaction ID// content ID//Kc//ACm//ACp} Kmc8, In the decoding processing section 5204, it is decoded by individual secret decode key Kmc8, and a license (license key Kc, transaction ID, content ID, the access restriction information ACm, and reproduction term ACp) is received (Step S172).
[0227]With reference to drawing 16, the controller 510 inputs into the license management device 520 the entry number for directing the entry which stores the license which the license management device 520 received (Step S174). So then, the controller 5220 of the license management device 520, An entry number is received via the terminal 5226 and the interface 5224, To the license area 5215B of the memory 5215 specified with the received entry number. The license (license key Kc, transaction ID, content ID, the access restriction information ACm, and reproduction term ACp) acquired in Step S172 is stored (Step S176).
[0228]The controller 510 of the personal computer 50 transmits transaction ID sent from the distributing server 10, and the distribution request of enciphered content data to the distributing server 10 (Step S178).
[0229]The distributing server 10 receives the distribution request of transaction ID and enciphered content data (Step S180), From the information database 304, enciphered content data {Dc} Kc and additional information Dc-inf are acquired, and these data is outputted via bus BS1 and the communication apparatus 350 (Step S182).
[0230]The personal computer 50 receives {Dc} Kc//Dc-inf, and receives enciphered content data {Dc} Kc and additional information Dc-inf (Step S184). If it does so, the controller 510 will record enciphered content data {Dc} Kc and additional information Dc-inf on the hard disk (HDD) 530 via bus BS2 as one contents file (Step S186). The entry number of the license with which the controller 510 was stored in the license management device 520, The license management file to enciphered content data {Dc} Kc and additional information Dc-inf containing transaction ID and content ID of a plaintext is generated, and it records on HDD530 via bus BS2 (Step S188). The controller 510 as information on the contents received to the contents list file currently recorded on HDD530, The name of the recorded contents file and a license management file, The information (a track name, an artist name) about the enciphered content data extracted from additional information Dc-inf, etc. are added (Step S190), and transaction ID and distribution acceptance are transmitted to the distributing server 10 (Step S192).

[0231]If transaction ID// distribution acceptance is received (Step S194), the distributing server 10, Record to storing of the billing data to the charge database 302 and the distribution recording data base 308 of transaction ID is performed, processing of the end of distribution is performed (Step S196), and the whole processing is completed (Step S198).
[0232]Thus, the license management device 50 built in the personal computer 50 is apparatus holding regular authentication data, After checking that open encryption key KPm7 which has enciphered and transmitted with class certificate Cm7 is effective simultaneously, Class certificate Cm7 can distribute contents data only to the distribution request from the license management device which is not written in prohibition class lists, i.e., the class certificate list in which encryption by open encryption key KPm7 was broken, The distribution using the class key to the inaccurate license management device distributed and decoded can be forbidden.
[0233]By exchanging the encryption key generated with a distributing server and a license management device, respectively, performing encryption using the encryption key which each received, and transmitting the encryption data to the other party, De facto mutual recognition can be performed also in transmission and reception of each encryption data, and the security of a data distribution system can be raised.
[0234]When the license management device 520 receives enciphered content data and a license from the distributing server 10, Since the license for exchanging data in hard between the distributing servers 10, and reproducing enciphered content data is stored in hard, the security level is high. Therefore, if the license management device 520 is used, while the personal computer 50 can receive enciphered content data and a license by high distribution of a security level, management of the level 2 license with a high security level is possible for it.
[0235][Distribution 2] In the data distribution system shown in drawing 1, the operation which distributes enciphered content data and a license to the license management module 511 of the personal computer 50 from the distributing server 10 is explained. This operation is called "distribution 2."
[0236]Drawing 17 - drawing 21 are the 1st for explaining the distribution operation to the license management module 511 built in the personal computer 50 by which it is generated at the time of the purchase of the enciphered content data in the data distribution system shown in drawing 1 - the 5th flow chart. The license management module 511 performs reception from enciphered content data and the distributing server 10 of a license by a program.
[0237]Before the processing in drawing 17, the user of the personal computer 50 connects via the modem 40 to the distributing server 10, and is premised on acquiring the content ID to the contents which wish to purchase.
[0238]With reference to drawing 17, the distribution request by specification of content ID is made via the keyboard 560 from the user of the personal computer 50 (Step S200). And the terms of purchase AC for purchasing the license of enciphered content data via the keyboard 560 are inputted (Step S202). That is, in order to purchase the license key Kc which decodes selected enciphered content data, the access restriction information ACm and the reproduction term ACp of enciphered content data are set up, and the terms of purchase AC are inputted.
[0239]When the terms of purchase AC of enciphered content data are inputted, the controller 510, Authentication data {KPm5//Cm5} KPa2 is read from the license management module 511, In addition to the authentication data {KPm5//Cm5} KPa2 read, the data AC and the distribution request of content ID and license terms of purchase are transmitted to the distributing server 10 (Step S204).
[0240]In the distributing server 10, from the personal computer 50 to a distribution

request. The data AC of content ID, authentication data {KPm5//Cm5} KPa2, and license terms of purchase is received (Step S206), Decoding processing is performed for the authentication data outputted from the license management module 511 in the decoding processing section 312 by level 1 authentication key KPa1 (Step S208).
[0241]The distribution control part 315 from the decoding processing result in the decoding processing section 312. Authenticating processing which judges whether the authentication data which gave the code for proving the justification of class public presentation encryption key KPm5 and class certificate Cm5 in whether processing was performed normally and a regular organization was received is performed (Step S210). When it is judged that it is just authentication data, the distribution control part 315 recognizes and receives class public presentation encryption key KPm5 and class certificate Cm5. And it shifts to the next processing (Step S212). In not being just authentication data, it is considered as non approval, and it ends processing without receiving class public presentation encryption key KPm5 and class certificate Cm5 (Step S288).
[0242]When it is recognized as a result of attestation that it is a regular module, the distribution control part 315, Next, it refers for whether class certificate Cm5 of the license management module 511 is listed by the prohibition class lists CRL to the CRL database 306, When these class certificates have been the targets of prohibition class lists, a distribution session is ended here (Step S288).
[0243]On the other hand, when the class certificate of the license management module 511 is outside the object of prohibition class lists, it shifts to the next processing (Step S214).
[0244]In [if it is checked that it is access from the personal computer provided with a license management module with just authentication data as a result of attestation, and a class is outside the object of prohibition class lists] the distributing server 10, The distribution control part 315 generates transaction ID which is the management codes for specifying distribution (Step S214). The session key generating part 316 generates session key Ks1 for distribution (Step S216). Session key Ks1 is enciphered by the enciphering processing part 318 by class public presentation encryption key KPm5 corresponding to the license management module 511 obtained by the decoding processing section 312 (Step S218).
[0245]Transaction ID and session key Ks1 which were enciphered are outputted outside via bus BS1 and the communication apparatus 350 as transaction ID//{Ks1} Km5 (Step S220).
[0246]With reference to drawing 18, the controller 510 of the personal computer 50, When transaction ID//{Ks1} Km5 are received (Step S222), the license management module 511, In response to the fact that {Ks1} Km5, decoding processing is carried out by class secret decode key Km5 [peculiar to the license management module 511], and session key Ks1 is received (Step S224).
[0247]The license management module 511 will generate session key Ks2, if acceptance of session key Ks1 generated with the distributing server 10 is checked (Step S226). And the controller 510 reads the encryption CRL memorized by HDD530 via bus BS2, and the license management module 511, Based on the prohibition class lists CRL which decoded the encryption CRL, and acquired and decoded the prohibition class lists CRL, the update date CRLdate of prohibition class lists is acquired (Step S228). Further the license management module 511 by session key Ks1 generated in the distributing server 10. The data CRLdate of session key Ks2 which made it generate by the license management module 511, individual public presentation encryption key KPmc6, and prohibition class lists is enciphered as one data row, and {Ks2//KPmc6//CRLdate} Ks1 is outputted (Step S230).

[0248]The controller 510 transmits transaction ID//{Ks2//KPmc6//CRLdate} Ks1 which added transaction ID to Ks2//KPmc6//encryption data {CRLdate} Ks1 to the distributing server 10 (Step S232).
[0249]The distributing server 10 receives transaction ID//{Ks2//KPmc6//CRLdate} Ks1 (Step S234), In the decoding processing section 320, decoding processing by session key Ks1 is performed, The update date CRLdate of the prohibition class lists in session key Ks2 generated by the license management module 511, individual public presentation encryption key KPmc6 [peculiar to the license management module 511], and the license management module 511 is received (Step S236).
[0250]The distribution control part 315 generates the access restriction information ACm and the reproduction term ACp according to the data AC of the content ID acquired at Step S206, and license terms of purchase (Step S238). The license key Kc for decoding enciphered content data is acquired from the information database 304 (Step S240).
[0251]The distribution control part 315 gives the generated license, i.e., transaction ID, content ID, license key Kc, the reproduction term ACp, and the access restriction information ACm to the enciphering processing part 326. The enciphering processing part 326, By individual public presentation encryption key KPmc6 [peculiar to the license management module 511 obtained by the decoding processing section 320], a license is enciphered and encryption data {transaction ID// content ID//Kc//ACm//ACp} Kmc6 is generated (Step S242).
[0252]With reference to drawing 19, in the distributing server 10 by the update date CRLdate of the prohibition class lists transmitted from the license management module 511. When it is judged whether the prohibition class lists CRL of the license management device 520 which has asked for distribution are the newest and the prohibition class lists CRL of a license management module are judged to be the newest, it shifts to Step S246. When it is judged that it is not the newest, it shifts to Step S252 (Step S244).
[0253]When judged as the newest, the enciphering processing part 328, Encryption data {transaction ID// content ID//Kc//ACm//ACp} Kmc6 outputted from the enciphering processing part 326 is enciphered by session key Ks2 generated in the license management module 511, Encryption data {{transaction ID// content ID//Kc//ACm//ACp} Kmc6} Ks2 is outputted to bus BS1. And the distribution control part 315 transmits encryption data {{transaction ID// content ID//Kc//ACm//ACp} Kmc6} Ks2 on bus BS1 to the personal computer 50 via the communication apparatus 350 (Step S246).
[0254]And the controller 510 of the personal computer 50, Encryption data {{transaction ID// content ID//Kc//ACm//ACp} Kmc6} Ks2 is received (Step S248), The license management module 511 decodes encryption data {{transaction ID// content ID//Kc//ACm//ACp} Kmc6} Ks2 by session key Ks2, {Transaction ID// content ID//Kc//ACm//ACp} Kmc6 is received (Step S250). Then, it shifts to Step S262.
[0255]On the other hand, if it is judged that it is not the newest, the distribution control part 315 will acquire the newest prohibition class lists CRL from the CRL database 306 via bus BS1, and will generate the difference CRL which is difference data (Step S252).
[0256]The enciphering processing part 328 is enciphered by session key Ks2 generated in the license management module 511 in response to the output of the enciphering processing part 326, and the difference CRL of the prohibition class lists which the distribution control part 315 supplies via bus BS1. Difference CRL/encryption data {/{transaction ID// content ID//Kc//ACm//ACp} Kmc6} Ks2 outputted from the enciphering processing part 328 is transmitted to the personal computer 50 via bus BS1 and the communication apparatus 350 (Step S254).

[0257]The personal computer 50 receives difference CRL/encryption data {/{transaction ID// content ID//Kc//ACm//ACp} Kmc6} Ks2 transmitted (Step S256), The license management module 511 decodes received data using session key Ks2, and receives them with the difference CRL and encryption data {transaction ID// content ID//Kc//ACm//ACp} Kmc6 (Step S258).
[0258]The controller 510 adds the difference CRL received to the prohibition class lists CRL recorded on HDD530, performs original cipher processing, and rewrites the prohibition class lists CRL in HDD530 (Step S260).
[0259]Step S246, S248, and S250 by the update date CRLdate of the prohibition class lists sent from the license management module 511. It is distribution operation to the license management module 511 of a license in case the prohibition class lists CRL which the license management module 511 manages are the newest, Step S252, S254, S256, S258, and S260 are distribution operations to the license management module 511 of a license in case the prohibition class lists CRL are not the newest. By thus, the update date CRLdate of the prohibition class lists sent from the license management module 511. When it checks in detail whether the prohibition class lists CRL of the license management device 520 which has asked for distribution are the newest and is not the newest, The license distributed to the license management module can be prevented from flowing into the apparatus by which security was broken by acquiring the newest prohibition class lists CRL from the CRL database 306, and distributing the difference CRL to the license management module 511.
[0260]Encryption license {transaction ID// content ID//Kc//ACm//ACp} Kmc6 after Step S250 or Step S260, It is decoded by individual secret decode key Kmc6, and a license (license key Kc, transaction ID, content ID, the access restriction information ACm, and reproduction term ACp) is received (Step S262).
[0261]Thus, by exchanging the encryption key generated by the distributing server and a license management module, respectively, performing encryption using the encryption key which each received, and transmitting the encryption data to the other party, De facto mutual recognition can be performed also in transmission and reception of each encryption data, and the security of a data distribution system can be raised.
[0262]The license management module 511 shifts to Step S266, when it distinguishes whether reproduction frequency is restricted and reproduction frequency is not restricted by the received access restriction information ACm, and when reproduction frequency is restricted, it shifts to Step S268 (Step S264). And it comes that reproduction frequency should be restricted and the license management module 511 generates the check-out information containing the number for lending out the enciphered content and the license which were received from the distributing server 10 to other devices which can be checked out (Step S266). In this case, the initial value of check-out is set as "3." When reproduction frequency is restricted, the license management module 511 sets as "0" the number for lending out enciphered content data to other devices which can be checked out, and generates check-out information (Step S268). Step S268 is processing for not performing management of reproduction frequency by checking out.
[0263]With reference to drawing 20, the license management module 511 outputs authentication data {KPm5//Cm5} KPa1 to the license management device 520 via the bus 2 after Step S266 or Step S268 (Step S270). In the license management device 520, from the license management module 511, receive and authentication data {KPm5//Cm5} KPa1 the decoding processing section 5208, Authentication data authentication data {KPm5//Cm5} KPa1 is received, Based on authentication data authentication data {KPm5//Cm5} KPa1, authentication data {KPm5//Cm5} KPa1 is decoded by level 1 authentication key KPa1 which received and received level 1 authentication key KPa1 from the KPa attaching part 5214 (Step S271).

[0264]The controller 5220 from the decoding processing result in the decoding processing section 5208. Authenticating processing which judges whether the authentication data which gave the code for proving the justification of class public presentation encryption key KPm5 and class certificate Cm5 in whether processing was performed normally and a regular organization was received is performed (Step S272). When it is judged that it is just authentication data, the controller 5220 recognizes and receives class public presentation encryption key KPm5 and class certificate Cm5. And it shifts to the next processing (Step S273). In not being just authentication data, it is considered as non approval, and it ends processing without receiving class public presentation encryption key KPm5 and class certificate Cm5 (Step S298).
[0265]When having received regular authentication data is recognized as a result of attestation, the controller 5220, Next, it refers for whether class certificate Cm5 of the license management module 511 is listed by the prohibition class lists CRL to the CRL field 5215A of the memory 5215, When these class certificates have been the targets of prohibition class lists, a distribution session is ended here (Step S298).
[0266]On the other hand, when the class certificate of the license management module 511 is outside the object of prohibition class lists, it shifts to the next processing (Step S273).
[0267]If it is checked that it is access from the license management module 511 provided with a license management device with just authentication data as a result of attestation, and a class is outside the object of prohibition class lists, In the license management device 520, the session key generating part 5208, Generating session key Ks2a (Step S274) the cipher-processing part 5210 enciphers session key Ks2a by class public presentation encryption key KPm5, and outputs encryption data [Ks2] {a} Km5 (Step S275).
[0268]The controller 5220 outputs encryption data [Ks2] {a} Km5 via bus BS5, the interface 5224, and the terminal 5226, and the license management module 511, Encryption data [Ks2] {a} Km5 is received via bus BS2, by class secret decode key Km5, encryption data [Ks2] {a} Km5 is decoded and session key Ks2a is received (Step S276). And the license management module 511, Session key Ks2b is generated (Step S277), session key Ks2b is enciphered by session key Ks2a, and encryption data {Ks2b} Ks2a is outputted to the license management device 520 via bus BS2 (Step S278).
[0269]The controller 5220 of the license management device 520, Receive encryption data {Ks2b} Ks2a via the terminal 5226, the interface 5224, and bus BS5, and the decoding processing section 5212, By session key Ks2a outputted from the session key generating part 5208, encryption data {Ks2b} Ks2a is decoded, and session key Ks2b is received (Step S279). So then, the license management module 511, Inputting the entry number "0" into the license management device 520 (Step S280) the controller 5220 of the license management device 520 receives the entry number "0" via the terminal 5226, the interface 5224, and bus BS5. The controller 5220 And the inside of the license area 5215B of the memory 5215, The binding license (the transaction IDb, content ID b, the binding key Kb, and the control information ACmb and ACpb) stored in the field specified with the entry number "0" is acquired (Step S281). And the controller 5220 distinguishes whether a binding license is effective based on the control information ACmb, when not effective, it shifts to Step S298 and a distribution session ends it. Here, since it is that the reproduction frequency within the control information ACmb is not 0, and the processing attested by level 1 authentication key KPa1, the case of being effective means that the security level of the control information ACmb is level 1.
[0270]On the other hand, when a binding license is effective, it shifts to Step S283 (Step S282).

[0271]When a binding license is judged to be effective, in Step S282 the cipher-processing part 5206, The binding key Kb and the control information ACpb which were acquired via the change-over switch 5246. It is decoded by the decoding processing section 5212, it enciphers with session key Ks2b acquired via the switch 5242, and encryption data [Kb//] {ACpb} Ks2b is outputted (Step S283).
[0272]With reference to drawing 21, the controller 5220, Output encryption data [Kb//] {ACpb} Ks2b via bus BS5, the interface 5224, and the terminal 5226, and the license management module 511, Encryption data [Kb//] {ACpb} Ks2b is received via bus BS2, with session key Ks2b, encryption data [Kb//] {ACpb} Ks2b is decoded, and the binding key Kb and the control information ACpb are acquired (Step S284).
[0273]A series of processings of Step S270 to the step S284 are processings which acquire the binding key Kb from the license management device 520, and are named "binding key acquisition processing" generically.
[0274]And the license management module 511 acquires the encryption confidential file 160 from HDD530 via bus BS2, decodes the acquired encryption confidential file 160 with the binding key Kb, and acquires the confidential file of a plaintext (Step S285). So then, the license management module 511, the license (transaction ID and content ID.) received from the distributing server 10 A postscript is added to the confidential file of a plaintext by making into the extra sensitive information n the zipper out information generated in license key Kc, the access restriction information ACm and the reproduction term ACp and Step S266, or Step S268 (Step S286). Then, the license management module 511 enciphers the confidential file of a plaintext again with the binding key Kb, and updates the encryption confidential file 160 recorded on HDD530 by the enciphered encryption confidential file 160 (Step S287). After storing a license in the encryption confidential file 160, the license management module 511 transmits transaction ID sent from the distributing server 10, and the distribution request of enciphered content data to the distributing server 10 (Step S288).
[0275]The distributing server 10 receives the distribution request of transaction ID and enciphered content data (Step S289), From the information database 304, enciphered content data {Dc} Kc and additional information Dc-inf are acquired, and these data is outputted via bus BS1 and the communication apparatus 350 (Step S290).
[0276]The license management module 511 receives {Dc} Kc//Dc-inf, and receives enciphered content data {Dc} Kc and additional information Dc-inf (Step S291). And the license management module 511 records enciphered content data {Dc} Kc and additional information Dc-inf on the hard disk (HDD) 530 as a contents file via bus BS2 (Step S292). The extra-sensitive-information number n of the extra sensitive information n which stored the license management module 511 in the encryption confidential file 160. The license management file corresponding to the contents file (enciphered content data {Dc} Kc and additional information Dc-inf) containing transaction ID and content ID of a plaintext is generated, and it records on HDD530 via bus BS2 (Step S293). The license management module 511, As contents information received to the contents list file currently recorded on HDD530, The name of the recorded contents file and a license management file, The information (a track name, an artist name) about the enciphered content data extracted from additional information Dc-inf, etc. are added (Step S294), and transaction ID and distribution acceptance are transmitted to the distributing server 10 (Step S295).
[0277]If transaction ID// distribution acceptance is received (Step S296), the distributing server 10, Record to storing of the billing data to the charge database 302 and the distribution recording data base 308 of transaction ID is performed, processing of the end of distribution is performed (Step S297), and the whole processing is completed (Step S298).

[0278]Thus, the license management module 511 exchanges data by software between the distributing servers 10, and receives enciphered content data and a license from the distributing server 10 in soft. The received enciphered content data is recorded on HDD530, it writes in a confidential file by making a license into the extra sensitive information n, the confidential file is enciphered with the binding key Kb, and a license is stored in the encryption confidential file 160. And the binding key Kb which decodes the encryption confidential file 160 is held at the license management device 520. Therefore, distribution of the enciphered content data based on the license management module 511, and a license, Although a security level is lower than distribution of the enciphered content data based on the license management device 520, and a license, in the point which is not related with the personal computer 50 in recording, it will become near it.
[0279][Ripping] The user of the personal computer 50 can acquire and use music data from the audio CD which enciphered content and a license are acquired by distribution, and also is owned. Although digital reproduction of an audio CD may not be freely performed from the position of an owner's of a copyright right protection, he is allowed for an individual to reproduce using a tool provided with a copyright protection function for the self purpose of use, and to enjoy music. Then, the license management module 511 acquires music data from an audio CD, and also includes the program which realizes the ripping function which generates enciphered content data manageable by the license management module 511, and a license.
[0280]There are some which inserted the electronic watermark called a watermark in music data in an audio CD in recent years. The range of use [in / in an owner of a copyright / a user] is written in this watermark as a use rule. It is necessary to certainly follow this use rule from a point of copyright protection in ripping from the music data in which the use rule is written in. Henceforth, they are duplicate conditions (it is assumed that duplication prohibition / time cost duplicate good / duplicate being possible" and the number of the maximum check-out are indicated.) as a use rule. In order to protect right of an owner of a copyright even if it is the conventional audio CD in which the use rule is not written when watermark detection is not carried out namely, the duplicate of time cost shall be made and the number of the maximum check-out shall interpret it as "3."
[0281]With reference to drawing 22 - drawing 24, acquisition of the enciphered content data based on ripping from the audio CD on which music data was recorded, and a license is explained.
[0282]Drawing 22 - drawing 24 are the 1st for acquiring enciphered content data and a license from an audio CD by ripping - the 3rd flow chart.
[0283]If ripping operation is started with reference to drawing 22, detection of the use rule which incorporated the music data which CD-ROM drive 540 detected from the audio CD, and was indicated with the watermark from the incorporated music data will be performed (Step S700). And it is judged whether it can reproduce based on the detected use rule (Step S701). When the duplicate conditions of a use rule are unrestricted, when a time cost duplicate of duplicate conditions is good, it shifts to Step S702 to Step S203, and when duplicate conditions are duplication prohibition, a duplicate is forbidden, it shifts to Step S733, and ripping operation is ended. When a watermark is not contained in CD with which it was equipped and a use rule is not acquired, it shifts to Step S705.
[0284]In Step S701, when a time cost duplicate of the duplicate conditions of a use rule is good, the license management module 511 is changed for the watermark which changed the duplicate conditions of the use rule which acquired the watermark contained in the acquired music data into duplication prohibition (Step S702). And it

shifts to Step S703. When the use rule which can do a duplicate is detected, in Step S703, the license management module 511 generates the access restriction information ACm and the reproduction term ACp reflecting a use rule (Step S703). According to duplicate conditions, if a duplicate is good, the move duplicate flags of the access restriction information ACm will be set up good [a move duplicate] (=3) also here, and if a time cost duplicate is good, since the ripping itself hits time cost, it will be set as move duplication prohibition (=0). Although there is no corresponding use rule, reproduction frequency is set as unlimitedness and a security level is set as level 1. Then, the license management ** module 511 sets up the number which can be checked out reflecting the number of the maximum check-out of a use rule. Specification of the number of the maximum check-out twists, and it is made into number =3 which can be checked out at the time. And the check-out information containing the set-up number which can be checked out is generated (Step S704).

[0285]When judged with a watermark not being detected but on the other hand there being no use rule in Step S701, the license management module 511, Move duplication prohibition (=0) and reproduction frequency being unrestricted (=255) and a security level set the move duplicate flags of the access restriction information ACm as 1. The reproduction term ACp makes reproduction indefinite (Step S705). Then, the license management module 511 generates the check-out information in which an initial value contains the number which is 3, and which can be checked out (Step S706).

[0286]After Step S704 or S706, a random number etc. are ****, and the license management module 511 generates the license key Kc (Step S707), and generates transaction ID and content ID of local use (Step S708). Next, the license management module 511 performs binding key acquisition processing. A series of processings of Step 723 of Step S709 of drawing 23 to drawing 24 are binding key acquisition processings, and it is the same as a series of processings of Step S284 of Step S270 of drawing 20 in the message distribution processing of the distribution 2 to drawing 21. Therefore, explanation is omitted.

[0287]With reference to drawing 24, the license management module 511 which acquired the binding key Kb, The encryption confidential file 160 is acquired from HDD530 via bus BS2, the acquired encryption confidential file 160 is decoded with the binding key Kb, and the confidential file of a plaintext is acquired (Step S724). So then, the license management module 511, The music data acquired from the audio CD is coded to a prescribed method, the contents data Dc is generated (Step S725), contents data is enciphered with the license key Kc, and enciphered content data {Dc} Kc is generated (Step S726). Then, the license management module 511, Based on the information from a user that it was inputted via the keyboard 560, and the information from an audio CD, Additional information Dc-inf of contents data is generated (Step S727), and enciphered content data {Dc} Kc and additional information Dc-inf are recorded on HDD530 as contents phi via bus BS2 (Step S728).

[0288]So then, the license management module 511, the generated license (transaction ID and content ID -- it license-key-Kc(ing) and) A postscript is added to the confidential file of a plaintext by making into the extra sensitive information n the check-out information generated in the access restriction information ACm and the reproduction term ACp and Step S704, or Step S706 (Step S729). Then, the license management module 511 enciphers the confidential file of a plaintext with the binding key Kb, and updates the encryption confidential file 160 recorded on HDD530 by the enciphered encryption confidential file 160 (Step S730). After storing a license in the encryption confidential file 160, the license management module 511, The extra-sensitive-information number n of the extra sensitive information n stored in the encryption confidential file 160. The license management file to the contents file

(enciphered content data {Dc} Kc and additional information Dc-inf) containing transaction ID and content ID of a plaintext is generated, and it records on HDD530 via bus BS2 (Step S731). The license management module 511, As information on the contents received to the contents list file currently recorded on HDD530, The name of the recorded contents file and a license management file, the information (a track name, an artist name) about the enciphered content data extracted from additional information Dc-inf, etc. are added (Step S732), and the whole processing is completed (Step S733).
[0289]Thus, enciphered content data and a license are acquirable from an audio CD also by ripping. And the enciphered content data and the license which were acquired by ripping from an audio CD are managed by the license management module 511 with the same method as the enciphered content data and the level 1 license which were acquired by distribution.
[0290]With reference to drawing 25, management of the enciphered content data received by the license management module 511 or the license management device 520 of the personal computer 50 and a license is explained. HDD530 of the personal computer 50 is provided with the following.
Contents list file 150.
The contents list files 150 are the contents files 1531-153n.
License management files 1521-152n.
Encryption confidential file.

[0291]The contents list file 150 is a data file of the list form of contents to own, and the information over each contents, including a musical piece name, an artist name, etc., the information (file name) which shows a contents file and a license management file, etc. are included. The information over each contents acquires required information from additional information Dc-inf at the time of reception, and is automatically indicated by a user's directions. Only a contents file can be managed in a list also about the contents which cannot reproduce only a license management file.
[0292]The contents files 1531-153n are files which record enciphered content data {Dc} Kc received by the license management module 511 or the license management device 520, and additional information Dc-inf, and are provided for every contents.
[0293]The license management files 1521-152n, Corresponding to the contents files 1531-153n, it is recorded, respectively, It is a file for managing the license received by the license management module 511 or the license management device 520, and the information about the information for pinpointing the storing position of a license and a license is included.
[0294]The information for pinpointing a storing position means an entry number or the extra-sensitive-information number which specifies the extra sensitive information recorded in the encryption confidential file, when a license is recorded on the license management device 520.
[0295]The information about a license is a copy of the plaintext of the matter restricted by transaction ID and content ID which can be referred to in a plaintext, and the access restriction information ACm and the reproduction control information ACp which can be easily judged from the license terms of purchase AC, when a license is received. It is protected and recorded until now that a license cannot be referred to because of contents protection so that clearly [explanation]. However, if it cannot even perform rewriting other information except the license key Kc, even if the contents are referred to, it is satisfactory in any way from the position of contents protection. In an application program, each processing is started with reference to the information about this license.
[0296]An encryption extra-sensitive-information file includes extra sensitive information including the license managed by the license management module 511,

check-out information, etc. The encryption extra-sensitive-information file is enciphered with the binding key Kb.
[0297]With reference to drawing 25, it explains concretely. The license management file 1521-1524 contains the entry number 1 and m, respectively. the license (license ID.) which this is received by the license management device 520 and managed in the license area 5215B of the memory 5215 of the license management device 520 It is a number which specifies the management domain of license key Kc, the access restriction information ACm, and the reproduction term ACm.
[0298]Therefore, when moving the enciphered content data of the file name recorded on the contents file 1531 to the memory card 110 equipped by the reproduction terminal 100, It is a solution or ** where if the contents files 1531-153n are searched and the contents file 1531 is extracted, the license which reproduces enciphered content data is managed Since the entry number contained in the license management file 1521 corresponding to the contents file 1531 is "1", The license which reproduces the enciphered content data of the file name recorded on the contents file 1531 is recorded on the field specified with the entry number 1 of the license area 5215B of the memory 5215 of the license management device 520. If it does so, the entry number 1 will be read from the license management file 1521 of the contents list file 150 recorded on HDD530, By inputting the read entry number 1 into the license management device 520, a license is easily taken out from the license area 5215B of the memory 5215, and it can move to the memory card 110. And since the license in the entry number 1 specified in the license area 5215B of the memory 5215 is deleted after moving a license, corresponding to it, "nothing [license]" is recorded like the license management file 1523.
[0299]The extra sensitive information which stores the license of the enciphered content data received with the license management module 511 is managed by the license management files 1522-1524, ..., 152n. The license management files 1522, ..., 152n include the extra-sensitive-information number of the extra sensitive information which stores the license for reproducing the enciphered content data received with the license management module 511.
[0300]When, moving the enciphered content data of the file name recorded on the contents file 1532 to the personal computer 80 so, then for example, The contents files 1531-153n are searched, the contents file 1532 is extracted, and the extra-sensitive-information number 1 is acquired from the license management file 1522 corresponding to the contents file 1532. On the other hand, the binding key Kb is acquired from the license management device 520, with the acquired binding key Kb, the encryption confidential file 160 is decoded and the confidential file of a plaintext is acquired. If it does so, the license stored in the extra sensitive information 1 in the confidential file corresponding to the extra-sensitive-information number 1 acquired from the license management file is acquirable.
[0301]Thus, in the embodiment of the invention 1, The license of the enciphered content data received with the license management module 511, It is stored in the encryption confidential file 160 as the extra sensitive information n, and the encryption confidential file 160 can be decoded only with the binding key Kb held in hard by the license management device 520. That is, the binding key Kb is a common key which manages the license of enciphered content data, and if there is no binding key Kb, it has structure which cannot acquire a license. Therefore, since the license of the enciphered content data received with the license management module 511 is written in the encryption confidential file 160 and recorded on HDD530, it is managed in soft in practice, but. If there is no binding key Kb stored in the license management device 520, since a license will be broken by the reason for the ability not to take out from the

encryption confidential file 160, substantially, it is close to being managed by hardware.
[0302]On the other hand, the license received by the license management device 520 is stored in the license area 5215B of the memory 5215. Therefore, the administered level of the license received by the embodiment of the invention 1 with the license management module 511 can be brought close to the administered level of the license received by the license management device 520.
[0303]The binding license is used as the thing stored in the entry number "0."
[0304][Movement 1] In the data distribution system shown in drawing 1, The operation which transmits the enciphered content data and the license which were distributed to the license management device 520 of the personal computer 50 from the distributing server 10 to the memory card 110 equipped by the reproduction terminal 100 is explained. This operation is called "movement 1." Drawing 26 whose security level of movement is the processing performed only between the levels 2 - drawing 29, In the data distribution system shown in drawing 1, they are the 1st for explaining the moving operation by which the license management device 520 moves the enciphered content data and the license which were received from the distributing server 10 to the memory card 110 equipped by the reproduction terminal 100 - the 4th flow chart.
[0305]Before the processing in drawing 18, the user of the personal computer 50, The contents which move are determined according to a contents list file, the contents file and license management file of HDD530 can be specified, and it explains acquiring the reproduction list file of the memory card 110 as a premise.
[0306]When a move request is inputted from the keyboard 560 of the personal computer 50 with reference to drawing 26 (Step S300), the controller 510, Request to Send a of authentication data is transmitted to the reproduction terminal 100 via USB interface 550, the terminal 580, and USB cable 70 (Step S302). So then, the controller 1106 of the reproduction terminal 100, The Request to Send of authentication data is received via terminal 1114, USB interface 1112, and bus BS3, and the Request to Send of authentication data is transmitted to the memory card 110 via bus BS3 and the memory card interface 1200. And the controller 1420 of the memory card 110 receives the Request to Send of authentication data via the terminal 1426, the interface 1424, and bus BS4 (Step S304).
[0307]The controller 1420 will read authentication data {KPm3//Cm3} KPa2 from the authentication data attaching part 1400 via bus BS4, if the Request to Send of authentication data is received, The authentication data {KPm3//Cm3} KPa2 read is outputted to the reproduction terminal 100 via bus BS4, the interface 1424, and the terminal 1426. And the controller 1106 of the reproduction terminal 100, Authentication data {KPm3//Cm3} KPa2 is received via the memory card interface 1200 and bus BS3, Authentication data {KPm3//Cm3} KPa2 is transmitted to the personal computer 50 via bus BS3, USB interface 1112, the terminal 1114, and USB cable 70 (Step S306).
[0308]So then, the controller 510 of the personal computer 50, Authentication data {KPm3//Cm3} KPa2 is received via the terminal 580 and USB interface 550 (Step S308), and the authentication data {KPm3//Cm3} KPa2 which received is transmitted to the license management device 520 via bus BS2. The controller 5220 of the license management device 520 receives authentication data {KPm3//Cm3} KPa2 via the terminal 5226, the interface 5224, and bus BS5, and gives the authentication data {KPm3//Cm3} KPa2 which received to the decoding processing section 5208. The authentication processing part 5208 the KPa attaching part 5214, Authentication data authentication data {KPm3//Cm3} KPa2 is received, Based on authentication data {KPm3//Cm3} KPa2, level 2 authentication-key KPa2 is received from the KPa attaching part 5214, and decoding processing of authentication data {KPm3//Cm3} KPa2 is performed by the level 2 authentication-key KPa2 received (Step S310). The

controller 5220 from the decoding processing result in the decoding processing section 5208. In order that whether processing having been performed normally and the memory card 110 may attest holding class public presentation encryption key KPm3 from a regular memory card, and class certificate Cm3, Authenticating processing which judges whether the authentication data which gave the code for proving the justification in a regular organization was received is performed (Step S312). When it is judged that it is just authentication data, the controller 5220 recognizes and receives class public presentation encryption key KPm3 and class certificate Cm3. And it shifts to the next processing (Step S314). In not being just authentication data, it is considered as non approval, and it ends processing without receiving class public presentation encryption key KPm3 and class certificate Cm3 (Step S404).

[0309]When it is recognized as a result of attestation that it is a regular memory card, the controller 5220, Next, it refers for whether class certificate Cm3 of the memory card 110 is listed by the prohibition class lists CRL to the CRL field 5215A of the memory 5215, When these class certificates have been the targets of prohibition class lists, moving operation is ended here (Step S404).

[0310]On the other hand, when the class certificate of the memory card 110 is outside the object of prohibition class lists, it shifts to the next processing (Step S314).

[0311]In [if it is checked that it is access from the reproduction terminal provided with a memory card with just authentication data as a result of attestation, and a class is outside the object of prohibition class lists] the license management device 520, The controller 5220 acquires transaction ID which is the management codes for specifying movement from the license area 5215B of the memory 5215 (Step S316). And the session key generating part 5218 generates session key Ks22 for movement (Step S318). Session key Ks22 is enciphered by the enciphering processing part 5210 by class public presentation encryption key KPm3 corresponding to the memory card 110 obtained by the decoding processing section 5208 (Step S320). The controller 5220 acquires encryption data {Ks22} Km3 via bus BS5, Transaction ID//{Ks22} Km3 which added transaction ID acquired from the memory 5215 to encryption data {Ks22} Km3 are outputted via bus BS5, the interface 5224, and the terminal 5226 (Step S322).

[0312]With reference to drawing 27, the controller 510 of the personal computer 50, Transaction ID//{Ks22} Km3 are received via bus BS2 (Step S324), Transaction ID//{Ks22} Km3 are transmitted to the reproduction terminal 100 via USB interface 550, the terminal 580, and USB cable 70 (Step S324). So then, the controller 1106 of the reproduction terminal 100, Transaction ID//{Ks22} Km3 are received via terminal 1114, USB interface 1112, and BS3, and its transaction ID// {Ks22} Km3 which received are transmitted to the memory card 110 via the memory card interface 1200. And the controller 1420 of the memory card 110 receives transaction ID//{Ks22} Km3 via the terminal 1426, the interface 1424, and bus BS4 (Step S326). The decoding processing section 1422 receives {Ks22} Km3 from the controller 1420 via bus BS4, by class secret decode key Km3 from the Km attaching part 1421, decodes {Ks22} Km3 and receives session key Ks22 (Step S328). And the session key generating part 1418 generates session key Ks2 (Step S330), and the controller 1420, The update date CRLdate of prohibition class lists is acquired from the CRL field 1415A of the memory 1415 via bus BS4, and the acquired update date CRLdate is given to the change-over switch 1446 (Step S332).

[0313]So then, session key Ks2 acquired when the enciphering processing part 1406 switched the terminal of the change-over switch 1446 one by one, individual public presentation encryption key KPmc4, and the update date CRLdate. It enciphers by session key Ks22 decoded by the decoding processing section 1404, and Ks2//KPmc4//encryption data {CRLdate} Ks22 are generated. The controller 1420

outputs Ks2//KPmc4//encryption data {CRLdate} Ks22 to the reproduction terminal 100 via bus BS4, the interface 1424, and the terminal 1426, The controller 1106 of the reproduction terminal 100 receives Ks2//KPmc4//encryption data {CRLdate} Ks22 via the memory card interface 1200. And the controller 1106 transmits to the personal computer 50 via USB interface 1112, the terminal 1114, and USB cable 70 (Step S334).
[0314]The controller 510 of the personal computer 50, Ks2//KPmc4//encryption data {CRLdate} Ks22 are received via the terminal 580 and USB interface 550 (Step S336), Ks2//KPmc4//encryption data {CRLdate} Ks22 are inputted into the license management device 520 via bus BS2 (Step S338). The controller 5220 of the license management device 520, Ks2//KPmc4//encryption data {CRLdate} Ks22 are received via the terminal 5226, the interface 5224, and bus BS5, and its Ks2//KPmc4// encryption data {CRLdate} Ks22 which received are given to the decoding processing section 5212. The decoding processing section 5212 decodes Ks2//KPmc4//encryption data {CRLdate} Ks22 by session key Ks22 from the session key generating part 5218, Session key Ks2, open encryption key KPmc4, and the prohibition class lists CRLdate are received (Step S340).
[0315]If it does so, the controller 510 of the personal computer 50 will read the entry number of the license included in a license management file from HDD530 in Step S324. And the controller 510 inputs the read entry number into the license management device 520 via bus BS2 (Step S342). The controller 5220 of the license management device 520, An entry number is received via the terminal 5226, the interface 5224, and bus BS5, A license (transaction ID, content ID, license key Kc, access-restriction-information ACm, reproduction term ACp) is read from the field specified with the entry number received in the license area 5215B of the memory 5215 (Step S344).
[0316]According to acceptance of the access restriction information ACm, the controller 5220 checks the access restriction information ACm (Step S346). That is, the controller 5220 judges the security level of the acquired access restriction information ACm, reproduction frequency, and move duplicate flags in order. First, based on the authentication key used at the security level and Step S310 of the access restriction information ACm, Since level 1 authentication key KPa1 is used, and it becomes an output to a security level lower than the management request level of a license when the security level of the access restriction information ACm is 2, it shifts to Step S404 and moving operation is stopped. It performs the next judgment, in being other. It is checked whether based on the reproduction frequency of the access restriction information ACm, the license which is going to move to the memory card 110 with which the reproduction terminal 100 was equipped is the license which cannot perform reproduction of enciphered content data by the access restriction information ACm. When reproduction frequency has become the restricted frequency by the access restriction information ACm (=0), It is because there is no meaning which moves to the memory card 110 which could not reproduce enciphered content data according to a license, but was equipped with the enciphered content data and license by the reproduction terminal 100. When reproduction frequency is "0", it shifts to Step S404 and moving operation is stopped. It performs the next judgment, in being other (reproduction frequency !=0). Based on the move duplicate flags of the access restriction information ACm, moving operation is stopped [step S404] at the time of move duplication prohibition "=0." when only movement is good, the controller 5220 deletes the license in the entry number specified in the license area 5215B of the memory 5215 [step S348] (Step S348" -- it is parallel step S350.) They are step S350 parallel at the time of move duplicate C "=2", without judging that it is a duplicate of a license and performing Step S348.

[0317]With reference to drawing 28, the enciphering processing part 5217, By individual public presentation encryption key KPmc4 [peculiar to the license management device 520] obtained by the decoding processing section 5212, a license is enciphered and encryption data {transaction ID// content ID//Kc//ACm//ACp} Kmc4 is generated (Step S350). And the license management device 520 compares the update date CRLdate transmitted from the memory card 110 with the update date of the prohibition class lists currently held to the CRL field 5215A, When it is judged whether which prohibition class lists are new and the direction of MEMOKADO 100 is judged to be new, it shifts to Step S352. When the direction of the license management device 520 is judged to be new, it shifts to Step S362 (Step S352).
[0318]When the data CRLdate is judged to be the newest, the enciphering processing part 5206, Encryption data {transaction ID// content ID//Kc//ACm//ACp} Kmc4 outputted from the enciphering processing part 5217 is enciphered by session key Ks2 generated in the session key generating part 5218, Encryption data {{transaction ID// content ID//Kc//ACm//ACp} Kmc4} Ks2 is outputted to bus BS5. And the controller 5220, Encryption data {{transaction ID// content ID//Kc//ACm//ACp} Kmc4} Ks2 on bus BS5 is transmitted to the personal computer 50 via the interface 5224 and the terminal 5226 (Step S354).
[0319]The controller 510 of the personal computer 50, Encryption data {{transaction ID// content ID//Kc//ACm//ACp} Kmc4} Ks2 is received, and it transmits to the reproduction terminal 100 via USB interface 550, the terminal 580, and USB cable 70 (Step S356).
[0320]The controller 1106 of the reproduction terminal 100 receives encryption data {{transaction ID// content ID//Kc//ACm//ACp} Kmc4} Ks2 via terminal 1114, USB interface 1112, and bus BS3, The encryption data {{transaction ID// content ID//Kc//ACm//ACp} Kmc4} Ks2 which received is transmitted to the memory card 110 via bus BS3 and the memory card interface 1200. And the controller 1420 of the memory card 110 receives encryption data {{transaction ID// content ID//Kc//ACm//ACp} Kmc4} Ks2 via terminal 1426, terminal 1424, and bus BS4 (Step S358).
[0321]The decoding processing section 1412 of the memory card 110, Encryption data {{transaction ID// content ID//Kc//ACm//ACp} Kmc4} Ks2 is received via bus BS4, It decodes by session key Ks2 generated by the session key generating part 1418, and {transaction ID// content ID//Kc//ACm//ACp} Kmc4 is received (Step S360). Then, it shifts to Step S376 shown in drawing 29.
[0322]When the direction of the license management device 520 is judged to be new, on the other hand in Step S350, the controller 5220 of the license management device 520, The newest prohibition class lists CRL are acquired from the CRL field 5215A of the memory 5215 via bus BS5 (Step S362).
[0323]The enciphering processing part 5206 the output of the enciphering processing part 5217, and the data CRL of the prohibition class lists which the controller 5220 acquired from the memory 5215 via bus BS5, Respectively, it receives via the change-over switches 5242 and 5246, and enciphers by session key Ks2 generated in the session key generating part 5218. It is outputted to the personal computer 50 via encryption data {CRL//{transaction ID// content ID / interface 5224 outputted from the enciphering processing part 5206, and the terminal 5226 (Step S364).
[0324]The controller 510 of the personal computer 50, Encryption data {CRL//{transaction ID// content ID//Kc//ACm//ACp} Kmc4} Ks2 outputted is received, Encryption data {CRL//{transaction ID// content ID//Kc//ACm//ACp} Kmc4} Ks2 is transmitted to the reproduction terminal 100 via USB interface 550, the terminal 580, and USB cable 70 (Step S368). The controller 1106 of the reproduction terminal 100

receives encryption data {CRL//{transaction ID// content ID//Kc//ACm//ACp} Kmc4} Ks2 via terminal 1114, USB interface 1112, and bus BS3, Encryption data {CRL//{transaction ID// content ID//Kc//ACm//ACp} Kmc4} Ks2 is transmitted to the memory card 110 via bus BS3 and the memory card interface 1200. And the controller 1420 of the memory card 110, Encryption data {CRL//{transaction ID// content ID//Kc//ACm//ACp} Kmc4} Ks2 is received via the terminal 1426, the interface 1424, and bus BS4 (Step S370).

[0325]In the memory card 110, the decoding processing section 1412, The received data on bus BS4 are decoded using session key Ks2 given from the session key generating part 1418, and CRL and {transaction ID// content ID//Kc//ACm//ACp} Kmc4 are received (Step 372). The controller 1420 receives the data CRL received by the decoding processing section 1412 via bus BS4, and rewrites the CRL field 1415A of the memory 1415 with the received data CRL (Step S374).

[0326]Step S354, S356, S358, and S360, The prohibition class lists CRL of the memory card 110 of the transmitting side from the prohibition class lists CRL of the license management device 520 of a receiver. Are the moving operation to the memory cards 110, such as the license key Kc in the case of being new, and Step S362, S364, S368, S370, S372, and S374, The prohibition class lists CRL of the license management device 520 of the transmitting side are the moving operation to the memory cards 110, such as the license key Kc in the case of being newer than the prohibition class lists CRL of the memory card 110 of a receiver. By thus, the update date CRLdate of the prohibition class lists sent from the memory card 110. By checking and making the more nearly newest prohibition class lists CRL store in the CRL field 1514A as the prohibition class lists CRL of the memory card 110 in detail, the license to the apparatus by which security functions, such as disclosure, were broken flows out, and a class secret key can prevent **.

[0327]With reference to drawing 29, with directions of the controller 1420 after Step S360 or Step S374. Encryption license {transaction ID// content ID//Kc//ACm//ACp} Kmc4, In the decoding processing section 1404, it is decoded by individual secret decode key Kmc4, and a license (license key Kc, transaction ID, content ID, the access restriction information ACm, and reproduction term ACp) is received (Step S376).

[0328]Thus, by exchanging the encryption key generated with a license management device and a memory card, respectively, performing encryption using the encryption key which each received, and transmitting the encryption data to the other party, De facto mutual recognition can be performed also in transmission and reception of each encryption data, and enciphered content data and the security in the moving operation of a license can be raised.

[0329]The controller 510 of the personal computer 50 transmits the entry number for storing the license which moved to the memory card 110 to the reproduction terminal 100 via USB interface 550, the terminal 580, and USB cable 70 (Step S378). So then, the controller 1106 of the reproduction terminal 100, An entry number is received via terminal 1114, USB interface 1112, and bus BS3, Transmit to the memory card 110 via bus BS3 and the memory card interface 1200, and the controller 1420 of the memory card 110, An entry number is received via the terminal 1426 and the interface 1424, To the license area 1415B of the memory 1415 specified with the received entry number. The license (license key Kc, transaction ID, content ID, the access restriction information ACm, and reproduction term ACp) acquired in Step S376 is stored (Step S380).

[0330]The controller 510 of the personal computer 50, The entry number of the license stored in the memory 1415 of the memory card 110, The license management file to enciphered content data {Dc} Kc and additional information Dc-inf which are going to

move to the memory card 110 containing transaction ID and content ID of a plaintext is generated, and it transmits to the memory card 110 (Step S382).
[0331]The controller 1420 of the memory card 110 records the license management file which received the license management file via the reproduction terminal 100, and received to the data area 1415C of the memory 1415 (Step S384).
[0332]And it is parallel step S390 without performing Step S388, if it will shift to Step S388 according to judgment of Step S346 if the controller 510 of the personal computer 50 is movement, and it is a duplicate (Step S386). And in movement, the license entry number of the license management file to the license which moved to the memory card 110 among the licenses recorded on HDD530 is updated to nothing [license] (Step S386).
[0333]Then, the controller 510 acquires from HDD530 the contents file (enciphered content data {Dc} Kc and additional information Dc-inf) which is going to move to the memory card 110, {Dc} Kc//Dc-inf is transmitted to the memory card 110 (Step S390). The controller 1420 of the memory card 110, It records on the data area 1415C of the memory 1415 by making into a contents file {Dc} Kc//Dc-inf which received {Dc} Kc//Dc-inf via the reproduction terminal 100 (Step S392), and received via bus BS4 (Step S394).
[0334]So then, the controller 510 of the personal computer 50, The reproduction list file which added the musical piece which moved to the memory card 110 is created (Step S396), and a reproduction list file and rewriting directions of a reproduction list file are transmitted to the memory card 110 (Step S398). The controller 1420 of the memory card 110, A reproduction list file and rewriting directions are received via the reproduction terminal 100 (Step S400), It rewrites to the reproduction list file which received the reproduction list file currently recorded on the data area 1415C of the memory 1415 via bus BS4 (Step S402), and moving operation is completed (Step S404).
[0335]With a reproduction list file, they are the contents list file currently recorded on HDD, and the management information file for reproduction terminals made from the same purpose. The reproduction terminal 100 is reproduced by specifying a contents file and a license management file in order of the appearance of the contents contained in this reproduction list file.
[0336]Thus, after checking that the memory card 110 with which the reproduction terminal 100 was equipped is regular apparatus, and that open encryption key KPm3 which has enciphered and transmitted with class certificate Cm3 is effective simultaneously, Class certificate Cm3 can move contents data only to the move demand to the memory card which is not written in prohibition class lists, i.e., the class certificate list in which encryption by open encryption key KPm3 was broken, Movement using the class key to the inaccurate memory card moved and decoded can be forbidden. By using this moving operation, the user of the reproduction terminal 102 who does not have a communication function with the distributing server 10 can also receive enciphered content data and a license to a memory card via the personal computer 50, and his convenience of a user improves.
[0337]Although it explained as moving processing that it was clear from explanation, when the duplicate of the license is permitted by the contents supplier, he performs as duplicate processing and a license is held as it is at the license management device 511 of the transmitting side. The duplicate in this case is not the act which was be each other an act permitted only when a contents supplier, i.e., a copyright person, permits a duplicate and he sets up the move duplicate flags of the access restriction information ACm good [a move duplicate] at the time of distribution, and checked the copyright person's right. access restriction information is a part of license, and the confidentiality is guaranteed -- **** -- it comes out and copyright is protected.

[0338]In the above, although movement of the license to the memory card 110 from the license management device 520 of the personal computer 50 was explained, Movement of a license to the license management device 520 from the memory card 110 is also performed according to the flow chart shown in drawing 26 - drawing 29. If the personal computer 50 can move the enciphered content data and the license which were received from the distributing server 10 to the memory card 110, The license management device 520 is only the enciphered content data and the license which were received in hard from the distributing server 10, The license management module 511 cannot transmit the enciphered content data and the license which were received in soft from the distributing server 10 to a memory card by the concept of "movement." The license management module 511 exchanges authentication data, an encryption key, etc. between the distributing servers 10 in soft with a security level lower than the license management device 520, Since enciphered content data and a license are received, a possibility that encryption will be broken in the receiving operation is higher than the case where the license management device 520 receives enciphered content data and a license. Therefore, the enciphered content data and the license which received with the low security level and were managed, Supposing it is freely movable to the memory card 110 which receives and manages enciphered content data and a license with the same security level as the license management device 520 by the concept of "movement", Since the security level in the memory card 110 falls, in order to prevent this, by the concept of "movement", it cannot transmit to the memory card 110 and the enciphered content data and the license which were received with the license management module 511 are carried out.
[0339]However, entirely, supposing the enciphered content data and the license with a low security level which were received with the license management module 511 are immovable to the memory card 110, It is contrary to the meaning of a data distribution system of permitting the free copy of contents data, protecting copyright, and a user's convenience does not improve, either. Then, it enabled it to transmit the enciphered content data and the license which were received with the license management module 511 to the memory card 110 by the concept of the check-out explained below and check-in.
[0340][Check-out] In the data distribution system shown in drawing 1, The operation which transmits the enciphered content data and the license which were distributed to the license management module 511 of the personal computer 50 from the distributing server 10 to the memory card 110 equipped by the reproduction terminal 100 is explained. This operation is called "check-out."
[0341]In the data distribution system shown in drawing 1, drawing 30 - drawing 34 the enciphered content data and the license which the license management module 511 received from the distributing server 10, They are the 1st for explaining the check-out operation lent out to the memory card 110 with which the reproduction terminal 100 was equipped on condition of return - the 5th flow chart. Before the processing in drawing 30, the user of the personal computer 50, The contents to check out are determined according to a contents list file, the contents file and license management file of HDD530 can be specified, and it explains acquiring the reproduction list file of the memory card 110 as a premise.
[0342]If a check-out request is inputted from the keyboard 560 of the personal computer 50 with reference to drawing 30 (Step S500), the license management module 511 will perform binding key acquisition processing. A series of processings of Step 515 of Step S501 of drawing 30 to drawing 31 are binding key acquisition processings, and it is the same as a series of processings of Step S284 of Step S270 of drawing 20 in the flow chart of the distribution 2 to drawing 21. Therefore, explanation is omitted.

[0343]The license management module 511 which acquired the binding key Kb, The encryption confidential file 160 is acquired from HDD530 via bus BS2, the acquired encryption confidential file 160 is decoded with the binding key Kb, and the confidential file of a plaintext is acquired (Step S516). Then, the license management module 511, The extra sensitive information n in the confidential file corresponding to the extra-sensitive-information number n recorded on the license management file (transaction ID, content ID, license key Kc, access-restriction-information ACm, the reproduction term ACp, and check-out information) is acquired (Step S517).
[0344]So then, the license management module 511, it is checked whether based on the acquired access restriction information ACm, he can check out a license (Step S518) -- it being got blocked and the license management module 511, It is checked whether it is the license with which whose reproduction restriction of the reproduction frequency of enciphered content data does not have the license which he is going to check out to the memory card 110 with which the reproduction terminal 100 was equipped by the reproduction frequency of the access restriction information ACm, or is impossible. When reproduction frequency has restriction, he does not check out enciphered content data and a license.
[0345]In Step S518, when reproduction has restriction, it shifts to Step S564 and check-out operation is ended. In Step S518, when the reproduction frequency of enciphered content data has not become the restricted frequency by the access restriction information ACm, it shifts to Step S519. And it is checked whether the license management module 511 has a number larger than "0" which is contained in the acquired check-out information and which can be checked out (Step S519). In Step S519, since there will be no license which can be checked out if the number which can be checked out is "0", it shifts to Step S564 and check-out operation is ended. In Step S519, when the number which can be checked out is larger than "0", the license management module 511 transmits the Request to Send of authentication data via USB interface 550, the terminal 580, and USB cable 70 (Step S520). The controller 1106 of the reproduction terminal 100 receives the Request to Send of authentication data via terminal 1114, USB interface 1112, and bus BS3, The Request to Send of authentication data which received is transmitted to the memory card 110 via bus BS3 and the memory card interface 1200. And the controller 1420 of the memory card 110 receives the Request to Send of authentication data via the terminal 1426, the interface 1424, and bus BS4 (Step S521).
[0346]The controller 1420 will read authentication data {KPm3//Cm3} KPa2 from the authentication data attaching part 1400 via bus BS4, if the Request to Send of authentication data is received, The authentication data {KPm3//Cm3} KPa2 read is outputted to the reproduction terminal 100 via bus BS4, the interface 1424, and the terminal 1426. And the controller 1106 of the reproduction terminal 100, Authentication data {KPm3//Cm3} KPa2 is received via the memory card interface 1200 and bus BS3, Authentication data {KPm3//Cm3} KPa2 is transmitted to the personal computer 50 via bus BS3, USB interface 1112, the terminal 1114, and USB cable 70 (Step S522).
[0347]So then, the license management module 511 of the personal computer 50, Authentication data {KPm3//Cm3} KPa2 is received via the terminal 580 and USB interface 550 (Step S523), and the authentication data {KPm3//Cm3} KPa2 which received is decoded by level 2 authentication-key KPa2 (Step S524).
[0348]With reference to drawing 32, the license management module 511, In order that whether processing having been performed normally and the memory card 110 may attest holding class public presentation encryption key KPm3 from a regular memory card, and class certificate Cm3 from a decoding processing result, Authenticating processing which judges whether the authentication data which gave the code for

proving the justification in a regular organization was received is performed (Step S525). When it is judged that it is just authentication data, the license management module 511 recognizes and receives class public presentation encryption key KPm3 and class certificate Cm3. And it shifts to the next processing (Step S526). In not being just authentication data, it is considered as non approval, and it ends processing without receiving class public presentation encryption key KPm3 and class certificate Cm3 (Step S564).

[0349]When it is recognized as a result of attestation that it is a regular memory card, the license management module 511, Next, when it refers for whether class certificate Cm3 of the memory card 110 is listed by the prohibition class lists CRL to HDD530 and these class certificates have been the targets of prohibition class lists about it, check-out operation is ended here (Step S564). On the other hand, when the class certificate of the memory card 110 is outside the object of prohibition class lists, it shifts to the next processing (Step S526).

[0350]If it is checked that it is access from the reproduction terminal provided with a memory card with just authentication data as a result of attestation, and a class is outside the object of prohibition class lists, The license management module 511 transaction ID for check-out which is the management codes for specifying check-out, A different value from all the transaction ID in which the memory card 110 is stored is taken, and it generates as transaction ID of local use. It generates (Step S527). And the license management module 511 generates session key Ks2b for check-out (Step S528), and generated session key Ks2b is enciphered by class public presentation encryption key KPm3 transmitted from the memory card 110 (Step S529). And the license management module 511, Transaction IDfor check-out//{Ks2b} Km3 which added transaction ID for check-out to encryption data {Ks2b} Km3 via USB interface 550, the terminal 580, and USB cable 70. It transmits to the reproduction terminal 100 (Step S530). So then, the controller 1106 of the reproduction terminal 100, Transaction IDfor check-out//{Ks2b} Km3 are received via terminal 1114, USB interface 1112, and bus BS3, Its transaction IDfor check-out// {Ks2b} Km3 which received are transmitted to the memory card 110 via the memory card interface 1200. And the controller 1420 of the memory card 110 receives transaction IDfor check-out//{Ks2b} Km3 via the terminal 1426, the interface 1424, and bus BS4 (Step S531). The decoding processing section 1422 receives {Ks2b} Km3 from the controller 1420 via bus BS4, by secret decode key Km3 from the Km attaching part 1421, decodes {Ks2b} Km3 and receives session key Ks2b (Step S532). And the session key generating part 1418 generates session key Ks2c (Step S533), and the controller 1420, The update date CRLdate of prohibition class lists is acquired from the CRL field 1415A of the memory 1415 via bus BS4, and the acquired update date CRLdate is given to the change-over switch 1446 (Step S534).

[0351]So Then, session key Ks2c acquired when the enciphering processing part 1406 switched the terminal of the change-over switch 1446 one by one, Individual public presentation encryption key KPmc4 and the update date CRLdate are enciphered with session key Ks2b decoded by the decoding processing section 1404, and Ks2c//KPmc4//encryption data {CRLdate} Ks2b is generated. The controller 1420 outputs Ks2c//KPmc4//encryption data {CRLdate} Ks2b to the reproduction terminal 100 via bus BS4, the interface 1424, and the terminal 1426, The controller 1106 of the reproduction terminal 100 receives Ks2c//KPmc4//encryption data {CRLdate} Ks2b via the memory card interface 1200. And the controller 1106 transmits to the personal computer 50 via USB interface 1112, the terminal 1114, and USB cable 70 (Step S535).

[0352]The license management module 511 of the personal computer 50, Ks2c//KPmc4//encryption data {CRLdate} Ks2b is received via the terminal 580 and USB interface 550 (Step S536), Received its Ks2c//KPmc4// encryption data

{CRLdate} Ks2b are decoded with session key Ks2b, and session key Ks2c and individual public presentation encryption key KPmc4 and the update date CRLdate are received (Step S537). And the license management module 511 generates the access restriction information ACm for check-out which forbade that a license should have been moved / reproduced to other memory cards from the memory card with which the reproduction terminal 100 was equipped. That is, a move duplicate of move duplicate flags being unrestricted (=255) and impossible (=3) and the access restriction information ACm which set the security level as 1 are generated for reproduction frequency (Step S538).

[0353]With reference to drawing 33, the license management module 511, By open encryption key KPmc4 [peculiar to the memory card 110 received in Step S537]. A license is enciphered and encryption data [ACm / transaction ID/for check-out / content ID//Kc// / for check-out//] {ACp} Kmc4 is generated (Step S539). And the update date CRLdate transmitted from the memory card 110. When it is judged whether which prohibition class lists are new and the direction of the memory card 110 is judged to be new as compared with the update date of the prohibition class lists held HDD530 which the license management module 511 manages, it shifts to Step S541. When the direction of the license management module 511 is conversely judged to be new, it shifts to Step S544 (Step S540).

[0354]When the direction of the memory card 110 is judged to be new, the license management module 511, Encryption data [ACm / transaction ID/for check-out / content ID//Kc// / for check-out//] {ACp} Kmc4 is enciphered by session key Ks2c, Transaction ID// content ID//Kc//encryption data {{ACm//ACpfor check-out for check-out} Kmc4} Ks2c via USB interface 550, the terminal 580, and USB cable 70. It transmits to the reproduction terminal 100 (Step S541).

[0355]The controller 1106 of the reproduction terminal 100, Transaction ID// content ID//Kc//encryption data {{ACm//ACpfor check-out for check-out} Kmc4} Ks2c is received via terminal 1114, USB interface 1112, and bus BS3, The transaction ID// content ID//Kc//encryption data {{ACm//ACpfor check-out for check-out} Kmc4} Ks2c which received is transmitted to the memory card 110 via bus BS3 and the memory card interface 1200. And the controller 1420 of the memory card 110, Transaction ID// content ID//Kc//encryption data {{ACm//ACpfor check-out for check-out} Kmc4} Ks2c is received via terminal 1426, terminal 1424, and bus BS4 (Step S542).

[0356]The decoding processing section 1412 of the memory card 110, Transaction ID// content ID//Kc//encryption data {{ACm//ACpfor check-out for check-out} Kmc4} Ks2c is received via bus BS4, It decodes by session key Ks2c generated by the session key generating part 1418, and transaction ID// content ID//Kc//{ACm//ACpfor check-out for check-out} Kmc4 are received (Step S543). Then, it shifts to Step S549 shown in drawing 34.

[0357]When the way of the prohibition class lists of the license management module 511 is judged to be new, on the other hand in Step S540, the license management module 511, The prohibition class lists CRL which the license management module 511 manages are acquired from HDD530 (Step S544).

[0358]And the license management module 511, Transaction ID// content ID//Kc//{ACm//ACpfor check-out for check-out} Kmc4, The data CRL of the prohibition class lists acquired from HDD530 is enciphered by session key Ks2c, The transaction ID// content ID//Kc//encryption data {CRL//{ACm//ACpfor check-out for check-out} Kmc4} Ks2c via USB interface 550, the terminal 580, and USB cable 70. It transmits to the reproduction terminal 100 (Step S545). The controller 1106 of the reproduction terminal 100, Transaction ID// content ID//Kc//encryption data

{CRL//{ACm//ACpfor check-out for check-out} Kmc4} Ks2c is received via terminal 1114, USB interface 1112, and bus BS3, The transaction ID// content ID//Kc//encryption data {CRL//{ACm//ACpfor check-out for check-out} Kmc4} Ks2c which received is outputted to the memory card 110 via bus BS3 and the memory card interface 1200. So then, the controller 1420 of the memory card 110, Transaction ID// content ID//Kc//encryption data {CRL//{ACm//ACpfor check-out for check-out} Kmc4} Ks2c is received via the terminal 1426, the interface 1424, and bus BS4 (Step S546).

[0359]In the memory card 110, the decoding processing section 1412, The received data on bus BS4 are decoded using session key Ks2c given from the session key generating part 1418, CRL, and transaction ID// content ID//Kc//{ACm//ACpfor check-out for check-out} Kmc4 are received (Step 547). The controller 1420 receives the data CRL received by the decoding processing section 1412 via bus BS4, and rewrites the CRL field 1415A of the memory 1415 with the received data CRL (Step S548).

[0360]Step S541, S542, and S543 from the prohibition class lists CRL of the license management module 511 of the transmitting side. It is check-out operation to the memory cards 110, such as the license key Kc when the prohibition class lists CRL of the memory card 110 of a receiver are new, Step S544, S545, S546, S547, and S548, It is check-out operation to the memory cards 110, such as the license key Kc when the prohibition class lists CRL of the license management module 511 of the transmitting side are newer than the prohibition class lists CRL of the memory card 110 of a receiver. From thus, the prohibition class lists CRL which the memory card 100 holds in the CRL field 1415B when transmitting a license to the memory card 110. By acquiring the prohibition class lists CRL from HDD530, when the new prohibition class lists CRL are recorded on HDD530, and distributing the prohibition class lists CRL to the memory card 110, The memory card 100 can prevent the outflow of the license which could forbid transmission to ****** to the memory card 110 in which the class key was torn, and was distributed which can update the prohibition class lists held in the CRL field 1415B.

[0361]With reference to drawing 34, with directions of the controller 1420 after Step S543 or Step S548. Encryption license [ACm / transaction ID/for check-out / content ID//Kc// / for check-out//] {ACp} Kmc4, In the decoding processing section 1404, it is decoded by secret decode key Kmc4 and a license (license key Kc, transaction ID for check-out, content ID, ACm for check-out, and reproduction term ACp) is received (Step S549).

[0362]And the license management module 511 of the personal computer 50, Via USB interface 550, the terminal 580, and USB cable 70, it transmits to the reproduction terminal 102 and the entry number for storing the license checked out to the memory card 110 is carried out (Step S550). So then, the controller 1106 of the reproduction terminal 102, An entry number is received via terminal 1114, USB interface 1112, and bus BS3, To the license area 1415B of the memory 1415 specified with the received entry number. The license (license key Kc, transaction ID for check-out, content ID, ACm for check-out, and reproduction control information ACp) received in Step S566 is stored (Step S551).

[0363]The license management module 511 of the personal computer 50, The entry number of the license stored in the memory 1415 of the memory card 110, The license management file to enciphered content data {Dc} Kc and additional information Dc-inf which are going to move to the memory card 110 containing transaction ID for check-out and content ID of a plaintext is generated, It transmits to the memory card 110 (Step S552).

[0364]The controller 1420 of the memory card 110 records the license management file

which received the license management file via the reproduction terminal 102, and received to the data area 1415C of the memory 1415 (Step S553).
[0365]The license management module 511 of the personal computer 50, The number which can be checked out is subtracted one time, transaction ID for check-out and open encryption key KPmc4 [peculiar to the memory card of a check-out place] are added, and check-out information is updated (Step S554). And the license management module 511, Transaction ID, content ID, address information that license-key-Kc(ed), access-restriction-information-ACm(ed), and it reproduction-term-ACp(ed), and was updated (with the number which can be checked out.) The confidential file of a plaintext is updated by making into the new extra sensitive information n what added individual door-to-door public presentation encryption key KPmc4 to transaction ID for check-out, and the memory card 110 of the check-out place (Step S555). Individual public key KPmc4 of a check-out place, an individual public key -- the Tampa-proof module of a memory card -- there is nothing -- since it has a characteristic value for every memory card which it is stored and comes to hand by the high means of communication of the security using the code by attestation, it is suitable as identification information which carries out memory card specification.
[0366]Then, the license management module 511 updates the encryption confidential file 160 which enciphers the confidential file of a plaintext with the binding key Kb, and is recorded on HDD530 (Step S556).
[0367]The license management module 511 acquires from HDD530 enciphered content data {Dc} Kc and additional information Dc-inf which he is going to check out to the memory card 110, and transmits {Dc} Kc//Dc-inf to the memory card 110 (Step S557). The controller 1420 of the memory card 110 records {Dc} Kc//Dc-inf which received {Dc} Kc//Dc-inf via the reproduction terminal 100 (Step S558), and received via bus BS4 on the data area 1415C of the memory 1415 (Step S559).
[0368]So then, the license management module 511 of the personal computer 50, The reproduction list file which added the musical piece checked out to the memory card 110 is created (Step S560), and the rewriting directions with a reproduction list file and a reproduction list file are transmitted to the memory card 110 (Step S561). The controller 1420 of the memory card 110, A regenerated list and rewriting directions are received via the reproduction terminal 100 (Step S562), It rewrites to the reproduction list file which received the reproduction list file currently recorded on the data area 1415C of the memory 1415 via bus BS4 (Step S563), and check-out operation is completed (Step S564).
[0369]Thus, after checking that the memory card 110 with which the reproduction terminal 100 was equipped is regular apparatus, and that class public presentation encryption key KPm3 enciphered and transmitted with class certificate Cm3 is effective simultaneously, Class certificate Cm3 can check out contents data only to the check-out demand to the memory card which is not written in prohibition class lists, i.e., the class certificate list in which encryption by class public presentation encryption key KPm3 was broken, The check-out using the class key to the inaccurate memory card checked out and decoded can be forbidden. By exchanging the encryption key generated with a license management module and a memory card, respectively, performing encryption using the encryption key which each received, and transmitting the encryption data to the other party, De facto mutual recognition can be performed also in transmission and reception of each encryption data, and enciphered content data and the security in check-out operation of a license can be raised. The user of the reproduction terminal 100 who does not have a communication function with the distributing server 10 by using this check-out operation, The personal computer 50 can receive the enciphered content data and the license which were received by software to a memory card, and

convenience's of a user improves.
[0370][Check-in] In the data distribution system shown in drawing 1, The operation which returns the enciphered content data and the license by which he was checked out from the license management module 511 of the personal computer 50 to the memory card 110 to the license management module 511 is explained. This operation is called "check-in."
[0371]Drawing 35 - drawing 38 are the 1st for explaining the check-in operation which returns and gets the enciphered content data and the license which were lent out to the memory card 110 by check-out operation explained with reference to drawing 30 - drawing 34 - the 4th flow chart. Before the processing in drawing 35, the user of the personal computer 50, The contents list file currently recorded on HDD520 and the reproduction list file currently recorded on the data area 1415B of the memory card 110 are acquired, It explains as a premise having determined the contents at which he checks in according to both files, and could specify the contents file and license management file of HDD530 and MEMOKADO 110, and acquiring the license management file of the memory card 110.
[0372]If a check-in request is inputted from the keyboard 560 of the personal computer 50 with reference to drawing 35 (Step S600), the license management module 511 will perform binding key acquisition processing. A series of processings of Step 615 of Step S601 of drawing 35 to drawing 36 are binding key acquisition processings, and it is the same as a series of processings of Step S284 of Step S270 of drawing 20 in the flow chart of the distribution 2 to drawing 21. Therefore, explanation is omitted.
[0373]The license management module 511 which acquired the binding key Kb, The encryption confidential file 160 is acquired from HDD530 via bus BS2, the acquired encryption confidential file 160 is decoded with the binding key Kb, and the confidential file of a plaintext is acquired (Step S616). Then, the license management module 511, the extra sensitive information n in the confidential file corresponding to the extra-sensitive-information number n recorded on the license management file (license (transaction ID.)) Content ID, license key Kc, access-restriction-information ACm, the reproduction term ACp, And check-out information (individual public presentation encryption key KPmcx of the memory card of the number which can be checked out, transaction ID for check-out, and a check-out place) is acquired (Step S617). And the license management module 511 transmits the Request to Send of authentication data to the reproduction terminal 100 via USB interface 550, the terminal 580, and USB cable 70 (Step S618).
[0374]So then, the controller 1106 of the reproduction terminal 100, The Request to Send of authentication data is received via terminal 1114, USB interface 1112, and bus BS3, and the Request to Send of authentication data is transmitted to the memory card 110 via bus BS3 and the memory card interface 1200. And the controller 1420 of the memory card 110 receives the Request to Send of authentication data via the terminal 1426, the interface 1424, and bus BS4 (Step S619).
[0375]The controller 1420 will read authentication data {KPm3//Cm3} KPa2 from the authentication data attaching part 1400 via bus BS4, if the Request to Send of authentication data is received, The authentication data {KPm3//Cm3} KPa2 read is outputted to the reproduction terminal 100 via bus BS4, the interface 1424, and the terminal 1426. And the controller 1106 of the reproduction terminal 100, Authentication data {KPm3//Cm3} KPa2 is received via the memory card interface 1200 and bus BS3, Authentication data {KPm3//Cm3} KPa2 is transmitted to the personal computer 50 via bus BS3, USB interface 1112, the terminal 1114, and USB cable 70 (Step S620).
[0376]The license management module 511 of the personal computer 50, Authentication data {KPm3//Cm3} KPa2 is received via the terminal 580 and USB

interface 550 (Step S621), and the authentication data {KPm3//Cm3} KPa2 which received is decoded with the level 2 authentication key KPa (Step S622). And the license management module 511, In order that whether processing having been performed normally and the memory card 110 may attest holding class public presentation encryption key KPm3 from a regular memory card, and class certificate Cm3 from a decoding processing result, Authenticating processing which judges whether the authentication data which gave the code for proving the justification in a regular organization was received is performed (Step S623). When it is judged that it is just authentication data, the license management module 511 recognizes and receives class public presentation encryption key KPm3 and class certificate Cm3. And it shifts to the next processing (Step S624). In not being just authentication data, it is considered as non approval, and it ends processing without receiving class public presentation encryption key KPm3 and class certificate Cm3 (Step S653). If it is recognized as a result of attestation that it is a regular memory card, the license management module 511 will generate straw-man transaction ID (Step S624). Transaction ID for straw men takes a certainly different value from all the transaction ID in which the memory card 110 is stored, and generates it as transaction ID of local use.

[0377]With reference to drawing 37, the license management module 511 generates session key Ks2b for check-in (Step S625). And the license management module 511, It enciphers by class public presentation encryption key KPm3 which received generated session key Ks2b from the memory card 110, Encryption data {Ks2b} Km3 is generated (Step S626), Straw-man transaction ID//{Ks2b} Km3 which added straw-man transaction ID to encryption data {Ks2b} Km3 are transmitted to the reproduction terminal 100 via USB interface 550, the terminal 580, and USB cable 70 (Step S627). The controller 1106 of the reproduction terminal 100 receives straw-man transaction ID//{Ks2b} Km3 via terminal 1114, USB interface 1112, and BS3, Its straw-man transaction ID// {Ks2b} Km3 which received are transmitted to the memory card 110 via the memory card interface 1200. And the controller 1420 of the memory card 110 receives straw-man transaction ID//{Ks2b} Km3 via the terminal 1426, the interface 1424, and bus BS4 (Step S628). The decoding processing section 1422 receives {Ks2b} Km3 from the controller 1420 via bus BS4, by class secret decode key Km3 from the Km attaching part 1421, decodes {Ks2b} Km3 and receives session key Ks2b (Step S629). And the session key generating part 1418 generates session key Ks2c (Step S630), and the controller 1420, The update date CRLdate of prohibition class lists is acquired from the CRL field 1415A of the memory 1415 via bus BS4, and the acquired update date CRLdate is given to the change-over switch 1446 (Step S631).

[0378]So Then, session key Ks2c acquired when the enciphering processing part 1406 switched the terminal of the change-over switch 1446 one by one, The decoding processing section 1422 decodes individual public presentation encryption key KPmc4 and the update date CRLdate, It enciphers with session key Ks2b acquired via terminal Pa of the change-over switch 1442, and Ks2c//KPmc4//encryption data {CRLdate} Ks2b is generated. The controller 1420 outputs Ks2c//KPmc4//encryption data {CRLdate} Ks2b to the reproduction terminal 100 via bus BS4, the interface 1424, and the terminal 1426, The controller 1106 of the reproduction terminal 100 receives Ks2c//KPmc4//encryption data {CRLdate} Ks2b via the memory card interface 1200. And the controller 1106 transmits Ks2c//KPmc4//encryption data {CRLdate} Ks2b to the personal computer 50 via USB interface 1112, the terminal 1114, and USB cable 70 (Step S632).

[0379]The license management module 511 of the personal computer 50, Ks2c//KPmc4//encryption data {CRLdate} Ks2b is received via the terminal 580 and USB interface 550 (Step S633), Received its Ks2c//KPmc4// encryption data

{CRLdate} Ks2b are decoded with session key Ks2b, and session key Ks2c and individual public presentation encryption key KPmc4 and the update date CRLdate are received (Step S634).

[0380]So then, the license management module 511, Whether it is the no contained in the check-out information on the extra sensitive information n which individual public presentation encryption key KPmc4 received acquired at Step S617, That is, it is checked whether it is in agreement with the individual public presentation encryption key KPmcx stored corresponding to transaction ID for check-out of the license which he is going to check out (Step S635).

[0381]Individual public presentation encryption key KPmc4 received is contained in the check-out information updated on the occasion of check-out of enciphered content data and a license (see Step S551 of drawing 34). Therefore, the check-out place checked out on the occasion of check-in can be easily specified by including individual public presentation encryption key KPmc4 corresponding to check-out places, such as enciphered content data, in check-out information.

[0382]In Step S635, when individual public presentation encryption key KPmc4 is not contained in check-out information, check-in operation is ended (Step S653). When individual public presentation encryption key KPmc4 is contained in check-out information, in Step S635 the license management module 511, A straw-man license, i.e., straw-man transaction ID, the corresponding straw-man content ID which does not recognize contents existence, The straw-man license key Kc (it expresses the straw man Kc.) which cannot participate in reproduction, The straw-man access restriction information ACm (it expresses the straw man ACm.) "move duplication prohibition" and reproduction frequency indicate "0" to be in move duplicate flags, And the straw-man reproduction term ACp (it expresses the straw man ACp.) is enciphered by individual public presentation encryption key KPmc4, and straw-man transaction ID// straw-man content ID//Kc// straw-man ACm/encryption data {/straw-man ACp} Kmc4 is generated (Step S636).

[0383]The license management module 511 enciphers straw-man transaction ID// straw-man content ID// straw-man Kc//straw-man ACm/encryption data {/straw-man ACp} Kmc4 by session key Ks2c, Straw-man transaction ID// straw-man content ID// straw-man Kc//straw-man ACm/encryption data {{/straw-man ACp} Kmc4} Ks2c is generated, The generated straw-man transaction ID// straw-man content ID//Kc// straw-man ACm/encryption data {{/straw-man ACp} Kmc4} Ks2c via USB interface 550, the terminal 580, and USB cable 70. It transmits to the reproduction terminal 100 (Step S637).

[0384]The controller 1106 of the reproduction terminal 100, Straw-man transaction ID// straw-man content ID// straw-man Kc//straw-man ACm/encryption data {{/straw-man ACp} Kmc4} Ks2c is received via terminal 1114, USB interface 1112, and bus BS3. The controller 1106, Straw-man transaction ID// straw-man content ID// straw-man Kc//straw-man ACm/encryption data {{/straw-man ACp} Kmc4} Ks2c which received is transmitted to the memory card 110 via bus BS3 and the memory card interface 1200. And the controller 1420 of the memory card 110, Straw-man transaction ID// straw-man content ID// straw-man Kc//straw-man ACm/{{/straw-man ACp} Kmc4} Ks2c is received via terminal 1426, terminal 1424, and bus BS4 (Step S638).

[0385]With reference to drawing 38, the decoding processing section 1412 of the memory card 110, Straw-man transaction ID// straw-man content ID// straw-man Kc//straw-man ACm/{{/straw-man ACp} Kmc4} Ks2c is received via bus BS4, It decodes by session key Ks2c generated by the session key generating part 1418, and straw-man transaction ID// straw-man content ID// straw-man Kc//straw-man ACm/{/straw-man ACp} Kmc4 is received (Step S639). And the decoding processing

section 1404 receives straw-man transaction ID// straw-man content ID// straw-man Kc//straw-man ACm/encryption data {/straw-man ACp} Kmc4 from the decoding processing section 1412, The straw-man transaction ID// straw-man content ID// straw-man Kc//straw-man ACm/encryption data {/straw-man ACp} Kmc4 received is decoded by individual secret decode key Kmc4 from the Kmc attaching part 1402, Straw-man transaction ID, straw-man content ID, the straw man Kc, the straw man ACm, and the straw man ACp are received (Step S640).

[0386]The license management module 511 of the personal computer 50, The entry number in which the license which is indicated to the license management file of the memory card 110, and to check out is stored is acquired, As an entry number for storing a straw-man license, it transmits to the reproduction terminal 102 via USB interface 550, the terminal 580, and USB cable 70 (Step S641). So then, the controller 1106 of the reproduction terminal 102, An entry number is received via terminal 1114, USB interface 1112, and bus BS3, To the license area 1415B of the memory 1415 specified with the received entry number via bus BS4. A straw-man license (straw-man transaction ID, straw-man content ID, straw-man license key Kc, the straw-man access restriction information ACm, and straw-man reproduction term ACp) is recorded (Step S642). Thus, the license checked out to the memory card 110 is eliminable by recording straw-man transaction ID, straw-man content ID, straw-man license key Kc, the straw-man access restriction information ACm, and the straw-man reproduction term ACp.

[0387]Then, the license management module 511 of the personal computer 50, Only 1 increases the number within check-out information which can be checked out, individual public key KPmc4 of the memory card of transaction ID for check-out and a check-out place is deleted, and check-out information is updated (Step S643). And the license management module 511 updates the confidential file of a plaintext by making into the new extra sensitive information n transaction ID, content ID, license key Kc, the access restriction information ACm, and the reproduction term ACp and the updated check-out information (Step S644). Then, the license management module 511 updates the encryption confidential file 160 which enciphers the confidential file of a plaintext with the binding key Kb, and is recorded on HDD530 (Step S645).

[0388]So then, the license management module 511, The deletion instruction which deletes the contents file (enciphered content data {Dc} Kc and additional information Dc-inf) and license management file corresponding to the license which is recorded on the data area 1415C of the memory card 100, and at which he checked in. It transmits to the reproduction terminal 100 via USB interface 550, the terminal 580, and USB cable 70 (Step S646). The controller 1106 of the reproduction terminal 100, The deletion instruction of a contents file (enciphered content data {Dc} Kc and additional information Dc-inf) and a license management file is received via terminal 1114, USB interface 1112, and bus BS3 (Step S647). If it does so, the controller 1106 will output the directions which delete (enciphered content data {Dc} Kc and additional information Dc-inf), and a license management file to the memory card 110, The controller 1420 of the memory card 110, The terminal 1426, the interface 1424, and the directions that delete enciphered content data {Dc} Kc and additional information Dc-inf, and a license management file via bus BS4 and to carry out are received, Enciphered content data {Dc} Kc and additional information Dc-inf, and the license management file of the memory 1415 are deleted via bus BS4 (Step S648).

[0389]The license management module 511 of the personal computer 50 creates the regenerated list which deleted the musical piece at which he checked in (Step S649), and transmits a regenerated list and rewriting directions of a regenerated list to the memory card 110 (Step S650). The controller 1420 of the memory card 110, It rewrites

to the regenerated list which received a regenerated list and rewriting directions via the reproduction terminal 100 (Step S651), and received the regenerated list of the memory 1415 via bus BS4 (Step S652), and check-in operation is completed (Step S653).
[0390]Thus, by returning and getting enciphered content data and a license from the partner point which checked out enciphered content data and a license, From the license management module with a low security level in which movement of a license is forbidden, and a license, Since the license which it was lent out to the memory card with a high security level, and was acquired by the license management module with a low security level in the memory card can be transmitted, Enciphered content data renewable according to the license acquired by the license management module with a low security level in the reproduction terminal can be reproduced and enjoyed.
[0391]The license lent out to the memory card, Since it is specified that it cannot output the license which checked out the memory card to other recording devices (a memory card, a license management device, and a license management module) by the access restriction information ACm, the lent-out license does not flow out. By checking in to the lent-out license management module <return>, the right of the lent-out license returns to the lent-out license management module. Therefore, a duplicate is not allowed to be made against an author's will, it is not the processing to which a security level falls, and copyright is also protected.
[0392][Reproduction] Next, the reproduction motion in the reproduction terminal 100 (it is [the following called contents playback device] the same) of the contents data which referred to drawing 39 and drawing 40 and in which he was moved and checked out by the memory card 110 is explained. Before the processing in drawing 29, the user of the reproduction terminal 102 determines the contents (musical piece) to reproduce according to a reproduction list file, specifies a contents file, and explains acquiring the license management file as a premise.
[0393]With reference to drawing 39, reproduction instruction is inputted to the reproduction terminal 100 via the navigational panel 1108 with the start of reproduction motion from the user of the reproduction terminal 100 (Step S1000). If it does so, the controller 1106 will read authentication data {KPp1//Cp1} KPa2 from the authentication data attaching part 1500 via bus BS3, Authentication data {KPp1//Cp1} KPa2 is outputted to the memory card 110 via the memory card interface 1200 (Step S1002).
[0394]If it does so, the memory card 110 will receive authentication data {KPp1//Cp1} KPa2 (Step S1004). And the decoding processing section 1408 of the memory card 110, Decoding authentication data {KPp1//Cp1} KPa2 received by level 2 authentication-key KPa2 held at the KPa attaching part 1414 (Step S1006) the controller 1420 performs authenticating processing from the decoding processing result in the decoding processing section 1408. That is, authentication data {KPp1//Cp1} KPa2 performs authenticating processing which judges whether it is regular authentication data (Step S1008). When it is not able to decode, it shifts to Step S1048 and reproduction motion is ended. When authentication data is able to be decoded, it is judged whether the controller 1420 is contained in the prohibition class lists CRL which class certificate Cp1 acquired read from the CRL field 1415A of the memory 1415 (Step S1010). In this case, the identification number is given to class certificate Cp1 and the controller 1420 distinguishes whether the identification number of received class certificate Cp1 exists in the prohibition class lists CRL. If it is judged that class certificate Cp1 is contained in prohibition class-lists data, it will shift to Step S1048 and reproduction motion will be ended.
[0395]In Step S1010, if it is judged that class certificate Cp1 is not contained in the prohibition class-lists data CRL, the session key generating part 1418 of the memory

card 110 will generate session key Ks2 for reproduction sessions (Step S1012). And the cipher-processing part 1410 outputs {Ks2} Kp1 which enciphered session key Ks2 from the session key generating part 1418 by class public presentation encryption key KPp1 decoded by the decoding processing section 1408 to bus BS3 (Step S1014). If it does so, the controller 1420 will output {Ks2} Kp1 to the memory card interface 1200 via the interface 1424 and the terminal 1426 (Step S1016). The controller 1106 of the reproduction terminal 100 acquires {Ks2} Kp1 via the memory card interface 1200. And the Kp1 attaching part 1502 outputs secret decode key Kp1 to the decoding processing section 1504.

[0396]By secret decode key Kp1 which was outputted from the Kp1 attaching part 1502 and which is open encryption key KPp1 and a pair, the decoding processing section 1504 decodes {Ks2} Kp1, and outputs session key Ks2 to the cipher-processing part 1506 (Step S1018). If it does so, the session key generating part 1508 will generate session key Ks3 for reproduction sessions, and will output session key Ks3 to the cipher-processing part 1506 (Step S1020). The cipher-processing part 1506 enciphers session key Ks3 from the session key generating part 1508 by session key Ks2 from the decoding processing section 1504, and outputs {Ks3} Ks2, The controller 1106 outputs {Ks3} Ks2 to the memory card 110 via bus BS3 and the memory card interface 1200 (Step S1022).

[0397]If it does so, the decoding processing section 1412 of the memory card 110 will input {Ks3} Ks2 via the terminal 1426, the interface 1424, and bus BS4 (Step S1024).

[0398]With reference to drawing 40, the decoding processing section 1412 decodes {Ks3} Ks2 by session key Ks2 generated by the session key generating part 1418, and receives session key Ks3 generated with the reproduction terminal 100 (Step S1026).

[0399]The controller 1106 of a reproduction terminal acquires the entry number in which the license is stored from the license management file of the reproduction request song beforehand acquired from the memory card 110, The entry number acquired to the memory card 110 via the memory card interface 1200 is outputted (Step S1027).

[0400]According to the input of an entry number, the controller 1420 checks the access restriction information ACm (Step S1028). In Step S1028, the access restriction information ACm which is information about the restriction to access of a memory specifically, It ends reproduction motion, in being in a state [that it is already unreproducible] by checking by checking reproduction frequency, It progresses to the following step, after updating the reproduction frequency of the access restriction information ACm (it reduces one), when the reproduction frequency of access restriction information has number-of-times restrictions (Step S1030). On the other hand, when reproduction frequency is not restricted by the reproduction frequency of the access restriction information ACm, Step S1030 is skipped, and processing advances to the following step (Step S1032), without updating the access restriction information ACm.

[0401]In Step S1028, when it is judged that it is renewable in the reproduction motion concerned, the license key Kc and the reproduction term ACp of a reproduction request song which were recorded on the license area 1415B of the memory 1415 are outputted on bus BS4 (Step S1032).

[0402]The license key Kc and the reproduction term ACp which were obtained are sent to the enciphering processing part 1406 via the point of contact Pf of the change-over switch 1446. The enciphering processing part 1406 enciphers the license key Kc which won popularity via the change-over switch 1446 by session key Ks3 received from the decoding processing section 1412 via the point of contact Pb of the change-over switch 1442, and the reproduction term ACp, {Kc//ACp} Ks3 is outputted to bus BS4 (Step S1034).

[0403]The encryption data outputted to bus BS4 is sent out to the reproduction terminal 100 via the interface 1424, the terminal 1426, and the memory card interface 1200.
[0404]In the reproduction terminal 100, the decoding processing section 1510 performs decoding processing for encryption data [Kc//] {ACp} Ks3 transmitted to bus BS3 via the memory card interface 1200, and the license key Kc and the reproduction term ACp are received (Step S1036). The decoding processing section 1510 transmits the license key Kc to the decoding processing section 1516, and outputs the reproduction term ACp to bus BS3.
[0405]Via bus BS3, the controller 1106 receives the reproduction term ACp and checks reproductive propriety (Step S1040).
[0406]In Step S1040, when it is judged by the reproduction term ACp that reproduction is impossible, reproduction motion is ended.
[0407]When it is judged in Step S1040 that it is refreshable, the controller 1106 requires enciphered content data {Dc} Kc recorded on the data area 1415C of the memory card 110 as a contents file via the memory card interface 1200. If it does so, the controller 1420 of the memory card 110 will acquire enciphered content data {Dc} Kc from the memory 1415, and will output it to the memory card interface 1200 via bus BS4, the interface 1424, and the terminal 1426 (Step S1042).
[0408]The controller 1106 of the reproduction terminal 100 acquires enciphered content data {Dc} Kc via the memory card interface 1200, and gives enciphered content data {Dc} Kc to the decoding processing section 1516 via bus BS3.
[0409]And the decoding processing section 1516 decodes enciphered content data {Dc} Kc with the contents key Kc outputted from the decoding processing section 1510, and acquires the contents data Data (Step S1044).
[0410]And the decoded contents data Dc is outputted to the music reproduction section 1518, the music reproduction section 1518 reproduces contents data, and DA converter 1519 changes a digital signal into an analog signal, and it outputs it to the terminal 1530. And from the terminal 1530, via an external output device, music data is outputted to the head telephone 130, and is reproduced (Step S1046). Reproduction motion is completed by this.
[0411]Although the case where the enciphered content data recorded on the memory card 110 was reproduced with the reproduction terminal 100 in the above was explained, It is possible to reproduce the enciphered content data received by the license management module 511 and the license management device 520 by building the contents playback device 1550 shown in drawing 7 in the personal computers 50 and 80. When reproducing the enciphered content data acquired with the license management module 511 with the contents playback device 1550, the license management module 511, The binding key Kb stored in the license management device 520 is acquired, the encryption confidential file 160 recorded on HDD530 is decoded with the binding key Kb, a license is read from the confidential file of a plaintext, and it gives to the contents playback device 1550.
[0412]It is possible to reproduce the enciphered content data which the license management module 511 acquired by software by building in the regenerating section which functions on the personal computers 50 and 80 according to the software which reproduces enciphered content data. Also in this case, the license management module 511, The binding key Kb stored in the license management device 520 is acquired, the encryption confidential file 160 recorded on HDD530 is decoded with the binding key Kb, a license is read from the confidential file of a plaintext, and it gives to the contents playback device 1550. Compared with the reproduction (level 2) using the contents playback device 1550 which has confidentiality in hard, since the reproduction by software is reproduction (level 1) which has confidentiality in soft, it is processing that a

security level is low. Therefore, the license held with the license management device 520 cannot be used by reproduction by this software.
[0413][Movement 2] In the data distribution system shown in drawing 1, the operation which moves the enciphered content data and the license which the license management module 511 of the personal computer 50 acquired to the personal computer 80 is explained. This movement is called [movement 2].
[0414]Drawing 41 - drawing 48 are the 1st for explaining movement in the enciphered content data which the license management module 511 acquired, and the personal computer 80 of a license - the 8th flow chart. Before the processing in drawing 41, the user of the personal computer 50, The contents which move are determined according to a contents list file, and it explains on the assumption that the contents file and license management file of HDD530 and MEMOKADO 110 specify. The natural number w which identifies the class of the license management module in the personal computer 80 of a receiver is w= 5, and the natural number y which identifies a license management module sets it to y= 5.
[0415]If the move request of the license acquired with the license management module 511 of the personal computer 50 via the keyboard 560 of the personal computer 50 is inputted with reference to drawing 41 (Step S800), The license management module 511 of the personal computer 50 performs binding key acquisition processing. A series of processings of Step 815 of Step S801 of drawing 41 to drawing 42 are binding key acquisition processings, and it is the same as a series of processings of Step S284 of Step S270 of drawing 20 in the flow chart of the distribution 2 to drawing 21. Therefore, explanation is omitted.
[0416]When a binding license is acquired, the license management module 511 of the personal computer 50, The encryption confidential file 160 is acquired from HDD530 via bus BS2, the acquired encryption confidential file 160 is decoded with the binding key Kb, and the confidential file of a plaintext is acquired (Step S816). Then, the license management module 511 of the personal computer 50, The extra sensitive information n in the confidential file corresponding to the extra-sensitive-information number n recorded on the license management file (transaction ID, content ID, license key Kc, access-restriction-information ACm, the reproduction term ACp, and check-out information) is acquired (Step S817).
[0417]So then, the license management module 511 of the personal computer 50, . Based on the acquired access restriction information ACm, check whether movement and the duplicate of enciphered content data are possible (Step S518). That is, the license management module 511, It is checked whether based on the reproduction frequency of the acquired access restriction information ACm, and move duplicate flags, the license which is going to move to the personal computer 80 is the license which cannot do movement and the duplicate of enciphered content data by the access restriction information ACm.
[0418]In Step S818, when movement and the duplicate of enciphered content data are forbidden, it shifts to Step S903 and moving operation is ended. In Step S818, when movement and the duplicate of enciphered content data are not forbidden, it shifts to Step S819. And it is checked whether based on the acquired check-out information, he can check out the license management module 511 (Step S819). In Step S819, since check-out is forbidden if check-out is impossible, it shifts to Step S903 and check-out operation is ended. In the device confirming processing which will perform device confirming processing in Step S819 in order to check whether a new binding key is storable in the license management device 520 if check-out is possible, Processing is interrupted, in order to maintain the actual condition when a new binding key cannot be recorded by the prohibition class lists CRL or it cannot attest the license management

device 520. A series of processings of Step 833 of Step S821 of drawing 42 to drawing 43 are device confirming processings, and it is the same as a series of processings of Step S42 of Step S16 of drawing 10 in the flow chart of initialization to drawing 11. Therefore, explanation is omitted.

[0419]After device confirming processing is completed, the license management module 511 of the personal computer 50 transmits the Request to Send of authentication data to the personal computer 80 via the telecommunication cable 90 (Step S834). If it does so, the license management module of the personal computer 80 will receive the Request to Send of authentication data (Step S835).

[0420]The license management module of the personal computer 80 will transmit authentication data {KPm5//Cm5} KPa1 to the personal computer 50, if the Request to Send of authentication data is received (Step S836). The license management module 511 of the personal computer 50, Authentication data {KPm5//Cm5} KPa1 is received via the terminal 580 and USB interface 550 (Step S837), and the authentication data {KPm5//Cm5} KPa1 which received is decoded by level 1 authentication key KPa1 (Step S838).

[0421]With reference to drawing 44, the license management module 511, In order that whether processing having been performed normally and the memory card 110 may attest holding class public presentation encryption key KPm5 from a regular memory card, and class certificate Cm5 from a decoding processing result, Authenticating processing which judges whether the authentication data which gave the code for proving the justification in a regular organization was received is performed (Step S839). When it is judged that it is just authentication data, the license management module 511 recognizes and receives open encryption key KPm3 and certificate Cm3. And it shifts to the next processing (Step S840). In not being just authentication data, it is considered as non approval, and it ends processing without receiving class public presentation encryption key KPm5 and class certificate Cm5 (Step S903). When it is recognized as a result of attestation that it is a regular memory card, the license management module 511, Next, when it refers for whether class certificate Cm3 of the memory card 110 is listed by the prohibition class lists CRL to HDD530 and these class certificates have been the targets of prohibition class lists about it, moving operation is ended here (Step S903). On the other hand, when the class certificate of the memory card 110 is outside the object of prohibition class lists, it shifts to the next processing (Step S840).

[0422]As a result of attestation, if it is checked that it is access from a reproduction terminal provided with a memory card with just authentication data, and a class is outside the object of prohibition class lists, the license management module 511 will generate session key Ks2d for movement (Step S841). And the license management module 511, It enciphers by class public presentation encryption key KPm5 which received generated session key Ks2d from the personal computer 80, Encryption data [Ks2] {d} Km5 is generated (Step S842), and transaction ID//{Ks2d} Km5 which added transaction ID to encryption data [Ks2] {d} Km5 is transmitted to the personal computer 80 via the telecommunication cable 90 (Step S843). The license management module of the personal computer 80 receives transaction ID//{Ks2d} Km5 (Step S844). And by class secret decode key Km3, the license management module of the personal computer 80 decodes {Ks2d} Km5, and receives session key Ks2d (Step S845). And the license management module of the personal computer 80 generates session key Ks2e (Step S846), and acquires the update date CRLdate of the prohibition class lists CRL from HDD (Step S847).

[0423]And the license management module of the personal computer 80, Session key Ks2e and individual public presentation encryption key KPmc5 and the prohibition class lists CRLdate are enciphered by session key Ks2d, Ks2e//KPmc5//encryption data

{CRLdate} Ks2d is generated, and Ks2e//KPmc5//encryption data {CRLdate} Ks2d is transmitted to the personal computer 50 via the telecommunication cable 90 (Step S848).
[0424]The license management module 511 of the personal computer 50, Ks2e//KPmc5//encryption data {CRLdate} Ks2d is received via the terminal 580 and USB interface 550 (Step S849), Received its Ks2e//KPmc5// encryption data {CRLdate} Ks2d are decoded by session key Ks2d, and session key Ks2e and individual public presentation encryption key KPmc5 and the update date CRLdate are received (Step S850). And the license management module 511, Transaction ID, content ID, license key Kc, the access restriction information ACm, And the reproduction term ACp is enciphered by individual public presentation encryption key KPmc5 [peculiar to the personal computer 80], and encryption data {transaction ID// content ID//Kc//ACm//ACp} Kmc5 is generated (Step S851).
[0425]With reference to drawing 45, the license management module 511 of the personal computer 50, Which of the prohibition class lists which the license management module of the personal computer 80 manages based on the update date CRLdate of the prohibition class lists transmitted from the license management module of the personal computer 80, and the prohibition class lists which self manages. When it judges whether it is new and it is judged that the prohibition class lists CRL which self manages are old, it shifts to Step S853. When the direction of the prohibition class lists CRL which self manages is conversely judged to be new, it shifts to Step S856 (Step S852).
[0426]When it is judged that the prohibition class lists CRL which self manages are old, the license management module 511, Encryption data {transaction ID// content ID//Kc//ACm//ACp} Kmc5 is enciphered by session key Ks2e generated in the license management module 511, Encryption data {{transaction ID// content ID//Kc//ACm//ACp} Kmc5} Ks2e is transmitted to the personal computer 80 via the telecommunication cable 90 (Step S853).
[0427]And the license management module of the personal computer 80, Encryption data {{transaction ID// content ID//Kc//ACm//ACp} Kmc5} Ks2e is received (Step S854), Encryption data {{transaction ID// content ID//Kc//ACm//ACp} Kmc5} Ks2e is decoded by session key Ks2e, {Transaction ID// content ID//Kc//ACm//ACp} Kmc5 is received (Step S855). Then, it shifts to Step S861.
[0428]On the other hand, in Step S852, if it is judged that the prohibition class lists CRL which self manages are new, the license management module 511 of the personal computer 50 will acquire the prohibition class lists CRL from HDD530 (Step S856). And the license management module 511, The prohibition class lists CRL and encryption data {transaction ID// content ID//Kc//ACm//ACp} Kmc5 are received, It enciphers by session key Ks2e, and encryption data {CRL//{transaction ID// content ID//Kc//ACm//ACp} Kmc5} Ks2e is transmitted to the personal computer 80 via the telecommunication cable 90 (Step S857).
[0429]The personal computer 80 receives transmitted encryption data {CRL//{transaction ID// content ID//Kc//ACm//ACp} Kmc5} Ks2e (Step S858), A license management module decodes received data using session key Ks2e, and receives them with CRL and encryption data {transaction ID// content ID//Kc//ACm//ACp} Kmc5 (Step S859).
[0430]The license management module of the personal computer 80 is rewritten by CRL which received the prohibition class lists CRL recorded on HDD (Step S860).
[0431]as for the prohibition class lists sent from the personal computer 80, update date CRLdate should boil Step S853, S854, and S855 -- ****, It is the moving operation to the personal computers 80, such as the license key Kc when inhibited class SURISUTO CRL which the personal computer 50 by the side of **** holds [the prohibition class

lists CRL which the personal computer 80 of a receiver holds] is newer, Step S854, S855, S856, S857, and S860, It is the moving operation to the personal computers 80, such as the license key Kc when inhibited class SURISUTO CRL which the personal computer 50 of the transmitting side holds [the prohibition class lists CRL which the personal computer 80 of a receiver holds] is older.

[0432]The license management module of the personal computer 80 after Step S855 or Step S860, Encryption data {transaction ID// content ID//Kc//ACm//ACp} Kmc5, It decodes by individual secret decode key Kmc5, and a license (license key Kc, transaction ID, content ID, the access restriction information ACm, and reproduction term ACp) is received (Step S861). And a license management module shifts to Step S863, when it distinguishes whether reproduction frequency is restricted and reproduction frequency is not restricted by the received access restriction information ACm, and when reproduction frequency is restricted, it shifts to Step S864 (Step S862). And it comes that reproduction frequency should be restricted and a license management module generates the check-out information containing the number for lending out the enciphered content and the license which were received from the personal computer 50 to other devices which can be checked out (Step S863). In this case, the initial value of check-out is set as "3." When reproduction frequency is restricted, a license management module sets as "0" the number for lending out enciphered content data to other devices which can be checked out, and generates check-out information (Step S864). Then, it shifts to Step S880 of drawing 46.

[0433]Rewriting operation of the binding license which the personal computer 50 holds in parallel to the personal computer 50 moving a license to the personal computer 80 is performed after Step S853 or Step S857. The license management module 511 of the personal computer 50 distinguishes whether the duplicate of a license is possible after Step S853 or Step S857 based on the access restriction information ACm (Step 865). And when the duplicate of a license is possible, it carries out henceforth to Step S898 of drawing 48, and enciphered content data {Dc} Kc and additional information Dc-inf are transmitted to the personal computer 80. When only movement is good, in Step S865, with the move decoding flag of the access restriction information ACm of a license the license management module 511, The license management file 152n of the contents list file 150 about the license which was recorded on HDD530 and to which it was made to move is read, the extra-sensitive-information number n recorded on the license management file is changed into nothing [license], the license management file 152n is updated (Step S866), and it differs from the binding key Kb which the beginning generated -- the binding key Kbb is newly generated (Step S867). And the extra sensitive information n in the confidential file of a plaintext is deleted, it enciphers with the binding key Kbb which newly generated the confidential file, and the license management module 511 updates the encryption confidential file 160 in HDD530 (Step S868).

[0434]With reference to drawing 46, since the newly generated binding key Kbb is stored in the license management device 520, the license management module 511 performs binding key registration processing of Step S869 to the step S879. It is the same processing as a series of processings of Step S66 of Step S44 of drawing 11 in the flow chart of initialization to drawing 12, and is [that session key Ks2b is only changed into the binding key Kbb with the new binding key Kb by session key Ks2c, and]. Therefore, explanation is omitted.

[0435]After registration of the new binding key Kbb is completed, it shifts to Step S898 of drawing 48.

[0436]With reference to drawing 47, acquisition of binding key Kb2 from the license management module to build in, i.e., the acquisition processing of a binding key, is

performed in the personal computer 80 after Step S861 of drawing 45, or Step S862. Also in the personal computer 80, it is the same as the personal computer 50, A series of processings in which it results [from Step S878] in the drawing 48 step S893 are binding key acquisition processings, It is the same as a series of processings in which it results [from Step S270 of drawing 20 in the flow chart of the distribution 2] in Step S284 of drawing 21, the binding license (transaction IDb2, the content ID b2, binding key Kb2 and control information ACmb2, ACpb2) to acquire -- session key Ks2a and Ks2b are [only being changed into Ks2g and Ks2f, respectively and]. Therefore, explanation is omitted.

[0437]When binding key Kb2 is acquired, the license management module of the personal computer 80, The encryption confidential file 160 is acquired from HDD530 via bus BS2, the acquired encryption confidential file 160 is decoded by binding key Kb2, and the confidential file of a plaintext is acquired (Step S895). then, the license (transaction ID.) which received the license management module from the personal computer 50 A postscript is added to the confidential file of a plaintext by making content ID, license key Kc, access-restriction-information ACm, the reproduction term ACp, and check-out information into the new extra sensitive information n2 (Step S896). And a license management module updates the encryption confidential file 160 which enciphers the confidential file of a plaintext by binding key Kb2, and is recorded on HDD (Step S897).

[0438]So then, the license management module 511 of the personal computer 50, After Step S868 and Step S897 of drawing 45 are completed [both], The contents file (enciphered content data {Dc} Kc and additional information Dc-inf) currently recorded on HDD530 is read, Enciphered content data {Dc} Kc and additional information Dc-inf are transmitted to the personal computer 80 via the telecommunication cable 90 (Step S898).

[0439]The license management module of the personal computer 80 receives enciphered content data {Dc} Kc and additional information Dc-inf, and receives enciphered content data {Dc} Kc and additional information Dc-inf (Step S899). And a license management module records on HDD enciphered content data {Dc} Kc and additional information Dc-inf which were received via bus BS2 as a contents file (Step S900). . A license management module contains the extra-sensitive-information number n2, transaction ID, and content ID. Enciphered content data {Dc} The license management file to the contents file which recorded Kc and additional information Dc-inf is created, and it records on HDD (Step S901). And a license management module adds the name of the contents received to the contents file of the contents list file currently recorded on HDD (Step S902), and moving operation ends it (Step S903).

[0440]Thus, by managing the license of the enciphered content data which the license management module 511 of the personal computer 50 acquired with the binding key Kb, Enciphered content data and a license are movable to the personal computer 80 from the personal computer 50.

[0441]Since the license of the enciphered content data which the license management module built in the personal computer acquired by software is managed with the binding key managed in hard by a license management device according to the Embodiment 1, It is possible to transmit enciphered content data and a license to other personal computers by the concept of "movement" like the license of the enciphered content data acquired by the license management device.

[0442][Embodiment 2] With reference to drawing 49, the controlling method in Embodiment 2 of a license of the enciphered content data acquired with the license management module 511 is explained.

[0443]The composition of the contents list file 150 is the same as the composition in

Embodiment 1. The encryption confidential file 160 is recorded on HDD530, and the transaction IDb stored in the license management device 520, content ID b, and the same thing as the binding key Kb are stored in this. And original encryption is given so that the encryption confidential file 160 may be carried out from the personal computer 50 depending on the serial number of CPU of the personal computer 50, etc. and it may become impossible. In the license management file to the license acquired with the license management module 511 among the license management files 1522, .., 152n, the license management files 1522 and 152n hit it. The plaintext information about the encryption extra sensitive information which enciphered similarly extra sensitive information including a license and check-out information as the encryption confidential file, and a license is included. A binding license is always stored in the entry number "0" of the license management device 520 to store.

[0444]The license management file to the license which stored the license in the license management device, the license management files 1521 and 152n change to the encryption extra sensitive information which hits this, and specify the entry to which the license area 1415B of a license management device licenses -- it is entry-number--ization-recorded. About other files and the composition of the license area 1415B, since it is the same as drawing 25 of Embodiment 1, explanation is omitted.

[0445]When taking out a license from the license management files 1522, .., 152n, If the license management files 1522, .., 152n are by encryption extra-sensitive-information ****, The entry number "0" is transmitted to the license management device 520, the binding key Kb is acquired from the license management device 520, and it checks that it is in agreement with the binding key Kb with which the acquired binding key Kb was stored in the encryption confidential file 160. If in agreement, encryption extra sensitive information will be decoded and a license and check-out information will be acquired. If not in agreement, since acquisition of a license is forbidden, it stops processing. On the other hand, when an entry number is contained, he leaves processing to the license management device 520. In the case of nothing [license], since a license does not exist, it stops processing. Therefore, in all the processings to Raisen [that a security level is low in this Embodiment 2 (level 1)], If the binding key Kb stored in the license management device 520 and the binding key Kb stored in the encryption confidential file 160 are not in agreement, the license of enciphered content data from the license management files 1522, .., 152n. It applies so that it cannot take out.

[0446]As a result, the license of the enciphered content data acquired with the license management module 511 also in this Embodiment 2, It can manage with the binding key Kb, and as Embodiment 1 explained, it becomes movable [the enciphered content data from the personal computer 50 to the personal computer 80, and a license].

[0447][Initialization] Drawing 50 - drawing 52 are the 1st for explaining initialization of the encryption confidential file 160 in Embodiment 2 - the 3rd flow chart. The flow chart shown in drawing 50 - drawing 52 replaces Step S66 of a flow chart with drawing 10 - drawing 12 at Step S66a, and is the same as the flow chart of drawing 10 - drawing 12 except it. Therefore, with reference to drawing 52 the license management module 511 after Step S64, The transaction IDb, content ID b, and the binding key Kb are stored in the confidential file of a plaintext, Encryption original with the confidential file of a plaintext is given, the encryption confidential file 160 is created, and the created encryption confidential file 160 is recorded on HDD530 (Step S66a). And operation of initialization is ended (Step S68).

[0448][Distribution 2] Drawing 53 - drawing 56 are the 1st for explaining operation when receiving enciphered content data and a license from the distributing server 10 from the license management module 511 - the 4th flow chart in Embodiment 2. The

flow chart shown in drawing 53 - drawing 56 replaces with step S287 a-S 287a Step S266 of the flow chart shown in drawing 17 - drawing 21, and the step between S268 and Step S288, and others are the same as the flow chart shown in drawing 17 - drawing 21. After check-out information is generated in Step S266 and S268 with reference to drawing 56, the license management module 511, Encryption original with the license (transaction ID, the content ID, license key Kc, the access restriction information ACm, and reproduction term ACp) and check-out information which were received, and binding information is given, and encryption extra sensitive information is generated (Step S286a). And the license management module 511 creates the license management file containing the encryption extra sensitive information, transaction ID, and content ID which were generated, and records it on HDD530 (Step S287a). Then, each step which shifted to Step S288 and was mentioned above is performed, and enciphered content data and distribution operation of a license are completed.

[0449][Ripping] Drawing 57 and drawing 58 are the 1st and 2nd flow charts for the license management module 511 to explain the operation of ripping which acquires enciphered content data and a license from an audio CD in Embodiment 2. The flow chart shown in drawing 57 and drawing 58, It is the same as the flow chart which replaces a step with Step S720a - Step S724a, and shows drawing 22 - drawing 24 the step between Step S708 of a flow chart and Step S725 which are shown in drawing 22 - drawing 24 except it. With reference to drawing 58, the license management module 511 after Step S708, Encryption original with the license (transaction ID, the content ID, license key Kc, the access restriction information ACm, and reproduction term ACp) and check-out information which were received, and binding information is given, and encryption extra sensitive information is generated (Step S723a). And the license management module 511 creates the license management file containing the encryption extra sensitive information, transaction ID, and content ID which were generated, and records it on HDD530 (Step S724a). Then, each step which shifted to Step S725 and was mentioned above is performed, and operation of enciphered content data and ripping of a license is completed.

[0450][Check-out] In Embodiment 2 drawing 59 - drawing 63, They are the 1st for explaining the operation which checks out the enciphered content data and the license which the license management module 511 acquired to the memory card 110 equipped by the reproduction terminal 100 - the 5th flow chart. The flow chart shown in drawing 59 - drawing 63 replaces with Step S516a, S516b, and S517a Step S516 of the flow chart shown in drawing 30 - drawing 34, and S517, Step S552 and S553 are replaced with Step S552a and 553a, and it is the same as the flow chart shown in drawing 30 - drawing 34 except it. With reference to drawing 60, the license management module 511 acquires the binding key Kb stored by acquiring the encryption confidential file 160 currently recorded on HDD530, and decoding after Step S515 (Step S516a). And the license management module 511, When it distinguishes whether it is in agreement with the binding key Kb which the binding key Kb acquired from the license management device 520 acquired from the encryption confidential file 160 and the two binding keys Kb are not mutually in agreement, It shifts to Step S564 and operation of check-out is ended. When the two binding keys Kb are mutually in agreement, it shifts to the following step S517a (Step S516b).

[0451]When in agreement with the binding key Kb which the binding key Kb acquired from the license management device 520 acquired from the encryption confidential file 160, Encryption extra sensitive information is acquired from the Raisen license management file, and the decoded license (license key Kc, transaction ID, content ID, the access restriction information ACm, and reproduction frequency ACp) is acquired (Step 517a). And with reference to drawing 63 which shifts to the following step S5118

the license management module 511 after Step S551, Encryption original with the extra sensitive information in which the updated check-out information was made to reflect is given, encryption extra sensitive information is generated (Step S552a), and a license management file including encryption extra sensitive information is updated (Step S553a). Then, each step which shifted to Step S554 and was mentioned above is performed, and operation of check-out of enciphered content data and a license is completed.

[0452]Thus, only when the binding key stored in the license management device 520 is in agreement with the binding key stored in the encryption confidential file 160, a license management module acquires the license of enciphered content data from a license management file. Therefore, also in Embodiment 2, the license of enciphered content data is substantially managed with a binding key.

[0453][Check-in] In Embodiment 2 drawing 64 - drawing 67, They are the 1st for explaining the operation which checks in at the enciphered content data and the license which the license management module 511 checked out to the memory card 110 with which the reproduction terminal 100 was equipped - the 4th flow chart. The flow chart shown in drawing 64 - drawing 67 replaces with Step S616a, and 616b and 617a Step S616 of the flow chart shown in drawing 35 - drawing 38, and S617, Step S643 and S644 are replaced with Step S643a and 644a, and it is the same as the flow chart shown in drawing 35 - drawing 38 except it.

[0454]With reference to drawing 65, the license management module 511 acquires the binding key Kb stored by acquiring the encryption confidential file 160 currently recorded on HDD530, and decoding after Step S615 (Step S616a). And the license management module 511, When it distinguishes whether it is in agreement with the binding key Kb which the binding key Kb acquired from the license management device 520 acquired from the encryption confidential file 160 and the two binding keys Kb are not mutually in agreement, It shifts to Step S653 and operation of check-in is ended. When the two binding keys Kb are mutually in agreement, it shifts to the following step S618 (Step S616b).

[0455]When in agreement with the binding key Kb which the binding key Kb acquired from the license management device 520 acquired from the encryption confidential file 160, Encryption extra sensitive information is acquired from a license management file, and the decoded license (license key Kc, transaction ID, content ID, the access restriction information ACm, and reproduction frequency ACp) is acquired (Step 617a). And it shifts to the following step S5118.

[0456]With reference to drawing 67, the license management module 511 after Step S642, Encryption original with the extra sensitive information in which the updated check-out information was made to reflect is given, encryption extra sensitive information is generated (Step S644a), and a license management file including encryption extra sensitive information is updated (Step S645a). Then, each step which shifted to Step S646 and was mentioned above is performed, and operation of check-in of enciphered content data and a license is completed.

[0457][Movement 2] In Embodiment 2 drawing 68 - drawing 74, They are the 1st for explaining the operation which moves the enciphered content data and the license which the license management module 511 received to the personal computer 80 from the personal computer 50 - the 7th flow chart. The flow chart shown in drawing 68 - drawing 74 inserts Step S800a - Step S800c between Step S800 of a flow chart and Step S801 which are shown in drawing 39 - drawing 46, The step between Step S815 and Step S820 is replaced with Step S816a and 817a, Step S867 is replaced with Step S867a and Step S867b, the step between Step S862, and S863 and Step S897 is replaced with Step S895a - 896a, and it is the same as the flow chart shown in drawing 39 - drawing

46 except it.
[0458]With reference to drawing 68, the license management module 511, The license management module 511 after Step S800, The encryption extra sensitive information of a license management file is decoded, and it is extra sensitive information (transaction ID, content ID, license key Kc, access-restriction-information ACm, the reproduction term ACp, and check-out information are acquired (Step S800a).). And the license management module 511 distinguishes whether movement and the duplicate of enciphered content data and a license are possible based on ACm acquired in Step S800a. And the license management module 511, When movement and the duplicate of enciphered content data and a license are forbidden, it shifts to Step S903, and it ends, and moving operation shifts to Step S800c, when movement and a duplicate are not forbidden (Step S800b).
[0459]the license management module 511 -- enciphered content data, when movement and the duplicate of b license are possible, It distinguishes whether he can check out based on check-out information, and when impossible, it shifts to Step S903, and it ends, and moving operation shifts to Step S801, when you can check out.
[0460]With reference to drawing 69, the license management module 511 acquires the binding key Kb stored by acquiring the encryption confidential file 160 currently recorded on HDD530, and decoding after Step S815 (Step S816a). And the license management module 511, When it distinguishes whether it is in agreement with the binding key Kb which the binding key Kb acquired from the license management device 520 acquired from the encryption confidential file 160 and the two binding keys Kb are not mutually in agreement, it shifts to Step S903 and operation of movement is ended. When the two binding keys Kb are mutually in agreement, it shifts to the following step S820 (Step S817a).
[0461]With reference to drawing 72, the license management module 511 after Step S867, The encryption confidential file which gave (Step S868a) and original encryption to rewriting at the binding key Kbb for the binding key Kb stored in the confidential file of division into equal parts is generated, and it rewrites with the encryption confidential file of HDD530 (Step S868b). Subsequently, it shifts to Step S869 of drawing 73.
[0462]After check-out information is generated in Step S862 and S863 with reference to drawing 74, the license management module 511, Encryption original with the license (transaction ID, the content ID, license key Kc, the access restriction information ACm, and reproduction term ACp) and check-out information which were received is given, and encryption extra sensitive information is generated (Step S895a). And the license management module 511 creates the license management file containing the encryption extra sensitive information, transaction ID, and content ID which were generated, and records it on HDD530 (Step S896a). Then, each step which shifted to Step S897 and was mentioned above is performed, and enciphered content data and distribution operation of a license are completed.
[0463]About other portions, it is the same as Embodiment 1. Since the license of the enciphered content data which the license management module built in the personal computer acquired by software is managed with the binding key managed in hard by a license management device according to the Embodiment 2, It is possible to transmit enciphered content data and a license to other personal computers by the concept of "movement" like the license of the enciphered content data acquired by the license management device.
[0464]Although it presupposed at operation that a binding license and the license by distribution are storable in the license management device 520 in the gestalten 1 and 2, you may be a management device only for a binding license.
[0465]In order to specify a binding license, the entry number was specified, but it may

have an entry for exclusive use, and you may treat in distinction from the license of a high level.

[0466]With all the points, the embodiment indicated this time is illustration and should be considered not to be restrictive. The range of this invention is shown by the above-mentioned not explanation but claim of an embodiment, and it is meant that all the change in a claim, an equivalent meaning, and within the limits is included.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]It is a schematic diagram which illustrates notionally the data distribution system in the embodiment of the invention 1.

[Drawing 2]It is a figure showing the characteristics, such as data for the communication in the data distribution system shown in drawing 1, and information.

[Drawing 3]It is a figure showing the characteristics, such as data for the communication in the data distribution system shown in drawing 1, and information.

[Drawing 4]It is a figure showing the characteristics, such as data for the communication in the data distribution system shown in drawing 1, and information.

[Drawing 5]It is a schematic block diagram showing the composition of the distributing server in the data distribution system shown in drawing 1.

[Drawing 6]It is a schematic block diagram showing the composition of the personal computer in the data distribution system shown in drawing 1.

[Drawing 7]It is a schematic block diagram showing the composition of the reproduction terminal in the data distribution system shown in drawing 1.

[Drawing 8]It is a schematic block diagram showing the composition of the memory card in the data distribution system shown in drawing 1.

[Drawing 9]It is a schematic block diagram showing the composition of the license management device built in the personal computer shown in drawing 6.

[Drawing 10]It is the 1st flow chart for explaining initialization of the confidential file in the personal computer shown in drawing 1.

[Drawing 11]It is the 2nd flow chart for explaining initialization of the confidential file in the personal computer shown in drawing 1.

[Drawing 12]It is the 3rd flow chart for explaining initialization of the confidential file in the personal computer shown in drawing 1.

[Drawing 13]It is the 1st flow chart for explaining high distribution operation of the security level in the data distribution system shown in drawing 1.

[Drawing 14]It is the 2nd flow chart for explaining high distribution operation of the security level in the data distribution system shown in drawing 1.

[Drawing 15]It is the 3rd flow chart for explaining high distribution operation of the security level in the data distribution system shown in drawing 1.

[Drawing 16]It is the 4th flow chart for explaining high distribution operation of the security level in the data distribution system shown in drawing 1.

[Drawing 17]It is the 1st flow chart for explaining low distribution operation of the security level in the data distribution system shown in drawing 1.

[Drawing 18]It is the 2nd flow chart for explaining low distribution operation of the security level in the data distribution system shown in drawing 1.

[Drawing 19]It is the 3rd flow chart for explaining low distribution operation of the security level in the data distribution system shown in drawing 1.

[Drawing 20]It is the 4th flow chart for explaining low distribution operation of the security level in the data distribution system shown in drawing 1.

[Drawing 21]It is the 5th flow chart for explaining low distribution operation of the security level in the data distribution system shown in drawing 1.
[Drawing 22]It is the 1st flow chart for explaining operation of ripping in the data distribution system shown in drawing 1.
[Drawing 23]It is the 2nd flow chart for explaining operation of ripping in the data distribution system shown in drawing 1.
[Drawing 24]It is the 3rd flow chart for explaining operation of ripping in the data distribution system shown in drawing 1.
[Drawing 25]It is a figure showing the composition of the contents list file in the hard disk of a personal computer.
[Drawing 26]It is the 1st flow chart for explaining the moving operation of a license of the enciphered content data in the data distribution system shown in drawing 1.
[Drawing 27]It is the 2nd flow chart for explaining the moving operation of a license of the enciphered content data in the data distribution system shown in drawing 1.
[Drawing 28]It is the 3rd flow chart for explaining the moving operation of a license of the enciphered content data in the data distribution system shown in drawing 1.
[Drawing 29]It is the 4th flow chart for explaining the moving operation of a license of the enciphered content data in the data distribution system shown in drawing 1.
[Drawing 30]It is the 1st flow chart for explaining check-out operation of a license of the enciphered content data in the data distribution system shown in drawing 1.
[Drawing 31]It is the 2nd flow chart for explaining check-out operation of a license of the enciphered content data in the data distribution system shown in drawing 1.
[Drawing 32]It is the 3rd flow chart for explaining check-out operation of a license of the enciphered content data in the data distribution system shown in drawing 1.
[Drawing 33]It is the 4th flow chart for explaining check-out operation of a license of the enciphered content data in the data distribution system shown in drawing 1.
[Drawing 34]It is the 5th flow chart for explaining check-out operation of a license of the enciphered content data in the data distribution system shown in drawing 1.
[Drawing 35]It is the 1st flow chart for explaining check-in operation of a license of the enciphered content data in the data distribution system shown in drawing 1.
[Drawing 36]It is the 2nd flow chart for explaining check-in operation of a license of the enciphered content data in the data distribution system shown in drawing 1.
[Drawing 37]It is the 3rd flow chart for explaining check-in operation of a license of the enciphered content data in the data distribution system shown in drawing 1.
[Drawing 38]It is the 4th flow chart for explaining check-in operation of a license of the enciphered content data in the data distribution system shown in drawing 1.
[Drawing 39]It is the 1st flow chart for explaining the reproduction motion in a reproduction terminal.
[Drawing 40]It is the 2nd flow chart for explaining the reproduction motion in a reproduction terminal.
[Drawing 41]It is the 1st flow chart for explaining movement between the enciphered content data in the data distribution system shown in drawing 1, and the personal computer of a license.
[Drawing 42]It is the 2nd flow chart for explaining movement between the enciphered content data in the data distribution system shown in drawing 1, and the personal computer of a license.
[Drawing 43]It is the 3rd flow chart for explaining movement between the enciphered content data in the data distribution system shown in drawing 1, and the personal computer of a license.
[Drawing 44]It is the 4th flow chart for explaining movement between the enciphered content data in the data distribution system shown in drawing 1, and the personal

computer of a license.
[Drawing 45]It is the 5th flow chart for explaining movement between the enciphered content data in the data distribution system shown in drawing 1, and the personal computer of a license.
[Drawing 46]It is the 6th flow chart for explaining movement between the enciphered content data in the data distribution system shown in drawing 1, and the personal computer of a license.
[Drawing 47]It is the 7th flow chart for explaining movement between the enciphered content data in the data distribution system shown in drawing 1, and the personal computer of a license.
[Drawing 48]It is the 8th flow chart for explaining movement between the enciphered content data in the data distribution system shown in drawing 1, and the personal computer of a license.
[Drawing 49]It is a figure showing other composition of the contents list file in the hard disk of a personal computer.
[Drawing 50]It is the 1st flow chart for explaining operation of everything but initialization of the confidential file in the personal computer shown in drawing 1.
[Drawing 51]It is the 2nd flow chart for explaining operation of everything but initialization of the confidential file in the personal computer shown in drawing 1.
[Drawing 52]It is the 3rd flow chart for explaining operation of everything but initialization of the confidential file in the personal computer shown in drawing 1.
[Drawing 53]It is the 1st flow chart for explaining other distribution operations with a low security level in the data distribution system shown in drawing 1.
[Drawing 54]It is the 2nd flow chart for explaining other distribution operations with a low security level in the data distribution system shown in drawing 1.
[Drawing 55]It is the 3rd flow chart for explaining other distribution operations with a low security level in the data distribution system shown in drawing 1.
[Drawing 56]It is the 4th flow chart for explaining other distribution operations with a low security level in the data distribution system shown in drawing 1.
[Drawing 57]It is the 1st flow chart for explaining operation of everything but ripping in the data distribution system shown in drawing 1.
[Drawing 58]It is the 2nd flow chart for explaining operation of everything but ripping in the data distribution system shown in drawing 1.
[Drawing 59]It is the 1st flow chart for explaining operation of everything but check-out of a license of the enciphered content data in the data distribution system shown in drawing 1.
[Drawing 60]It is the 2nd flow chart for explaining operation of everything but check-out of a license of the enciphered content data in the data distribution system shown in drawing 1.
[Drawing 61]It is the 3rd flow chart for explaining operation of everything but check-out of a license of the enciphered content data in the data distribution system shown in drawing 1.
[Drawing 62]It is the 4th flow chart for explaining operation of everything but check-out of a license of the enciphered content data in the data distribution system shown in drawing 1.
[Drawing 63]It is the 5th flow chart for explaining operation of everything but check-out of a license of the enciphered content data in the data distribution system shown in drawing 1.
[Drawing 64]It is the 1st flow chart for explaining operation of everything but check-in of a license of the enciphered content data in the data distribution system shown in drawing 1.

[Drawing 65]It is the 2nd flow chart for explaining operation of everything but check-in of a license of the enciphered content data in the data distribution system shown in drawing 1.
[Drawing 66]It is the 3rd flow chart for explaining operation of everything but check-in of a license of the enciphered content data in the data distribution system shown in drawing 1.
[Drawing 67]It is the 4th flow chart for explaining operation of everything but check-in of a license of the enciphered content data in the data distribution system shown in drawing 1.
[Drawing 68]It is the 1st flow chart for explaining other movements between the enciphered content data in the data distribution system shown in drawing 1, and the personal computer of a license.
[Drawing 69]It is the 2nd flow chart for explaining other moving operation between the enciphered content data in the data distribution system shown in drawing 1, and the personal computer of a license.
[Drawing 70]It is the 3rd flow chart for explaining other moving operation between the enciphered content data in the data distribution system shown in drawing 1, and the personal computer of a license.
[Drawing 71]It is the 4th flow chart for explaining other moving operation between the enciphered content data in the data distribution system shown in drawing 1, and the personal computer of a license.
[Drawing 72]It is the 5th flow chart for explaining other moving operation between the enciphered content data in the data distribution system shown in drawing 1, and the personal computer of a license.
[Drawing 73]It is the 6th flow chart for explaining other moving operation between the enciphered content data in the data distribution system shown in drawing 1, and the personal computer of a license.
[Drawing 74]It is the 7th flow chart for explaining other moving operation between the enciphered content data in the data distribution system shown in drawing 1, and the personal computer of a license.
[Description of Notations]
10 A distributing server and 20 A distribution career, 30 Internet networks, 40 A modem, and 50 and 80 A personal computer, 60 CD, 70 A USB cable, 90 telecommunication cables, and 100 A reproduction terminal and 110 Memory card, 130 head telephones and 150 A contents list file and 160 Encryption confidential file, 302 A charge database, 304 information databases, a 306 CRL database, 307 A menu database and 308 A distribution recording data base, 310 data processing parts, 312,320,1404, 1408,1412,1422, 1504,1510,1516, 5204,5208,5212, and 5222 Decoding processing section, 313 An authentication key attaching part and 315 A distribution control part, 316, a session key generating part, 318, 326, 328, 1406, 1410, 1417, 1506, 5206, 5210, 5217, and 5405 Cipher-processing part, 350 A communication apparatus, 510-1106 and 1420, 5220 controllers, a 511 license-management module, a 520 license-management device, and 530 A hard disk, 540 CD-ROM drives, 550-1112 USB interfaces and 560 A keyboard and 570 Display, 580-1114, 1426, 1530, and 5226 A terminal, 1108 navigational panels, 1110 A display panel and 1200 A memory card interface, 1400-1500, a 5200 authentication-data attaching part, A 1402-5202 Kmc attaching part, a 1414-5214 KPa attaching part, 1415-5215 A memory, a 1415 A-5215A CRL field, A 1415 B-5215B license area, a 1415C data area, A 1416-5216 KPmc attaching part and 1418-5218 Session key generating part, A 1421-5221 Km attaching part and 1424-5224 Interface, 1442-1446 change-over switches, 1502 Kp1 attaching part, and 1518 A music reproduction section, 1519 DA converters, a 1521-152n license management file, and

1531-153n A contents file, 1550 contents-playback device.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－164881
（P2002－164881A）
(43)公開日　平成14年６月７日(2002.6.7)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード*（参考）
Ｈ０４Ｌ　9/08		Ｃ０６Ｆ　13/00	５４０Ｓ	５Ｊ１０４
Ｇ０６Ｆ　13/00	５４０	Ｃ０９Ｃ　1/00	６６０Ａ	
Ｇ０９Ｃ　1/00	６６０		６６０Ｄ	
		Ｈ０４Ｌ　9/00	６０１Ｂ	
Ｈ０４Ｌ　9/32			６０１Ａ	

審査請求　未請求　請求項の数27　ＯＬ　（全109頁）　最終頁に続く

(21)出願番号　特願2000－362913(P2000－362913)

(22)出願日　平成12年11月29日(2000.11.29)

(71)出願人　000001889
三洋電機株式会社
大阪府守口市京阪本通２丁目５番５号

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号

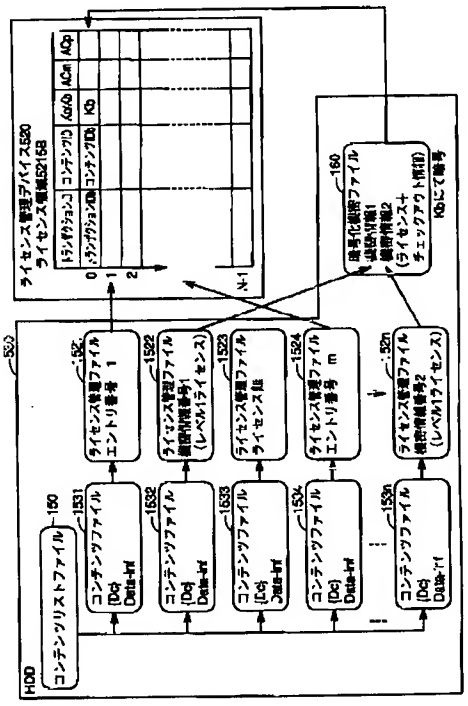
(71)出願人　000136136
株式会社ピーエフユー
石川県河北郡宇ノ気町字宇野気ヌ98番地の２

(74)代理人　100064746
弁理士　深見　久郎　（外３名）

最終頁に続く

(54)【発明の名称】　データ端末装置

(57)【要約】
【課題】　ソフトウエアによって配信された暗号化コンテンツデータおよびライセンスを他のデータ端末装置へ移動可能なデータ端末装置を提供する。
【解決手段】　パーソナルコンピュータのハードディスク５３０は、コンテンツリストファイル１５０と暗号化機密ファイル１６０とを有する。ライセンス管理デバイス５２０は、メモリのライセンス領域５２１５Ｂにバインディング鍵Ｋｂを格納する。暗号化機密ファイル１６０は、ライセンス管理デバイス５２０に格納されたバインディング鍵Ｋｂによって復号および暗号化が可能である。そして、取得された暗号化コンテンツデータのライセンスは、暗号化機密ファイル１６０に機密情報として格納される。



【特許請求の範囲】

【請求項１】　コンテンツデータを暗号化した暗号化コンテンツデータおよび前記暗号化コンテンツデータを復号して元の平文を得るためのライセンスを取得し、前記暗号化コンテンツデータおよび前記ライセンスを他のデータ端末装置へ出力するデータ端末装置であって、
前記暗号化コンテンツデータおよび前記ライセンスをソフトウエアによって取得するモジュール部と、
前記暗号化コンテンツデータと、ライセンス管理ファイルと、暗号化機密ファイルとを記憶する記憶部と、
前記暗号化機密ファイルを復号し、かつ、その復号した機密ファイルを暗号化するバインディング鍵を含むバインディングライセンスを専用領域に格納するデバイス部とを備え、
前記機密ファイルは、前記ライセンスを構成要素とする機密情報を含み、
前記ライセンス管理ファイルは、前記暗号化コンテンツファイルに対応し、かつ、前記機密ファイルに含まれる前記機密情報の管理番号を含む、データ端末装置。

【請求項２】　前記暗号化機密ファイルの初期化時、
前記モジュール部は、前記バインディング鍵を含めて前記バインディングライセンスを生成し、機密情報が空な機密ファイルを生成し、その生成した機密ファイルを前記生成したバインディング鍵によって暗号化して前記暗号化機密ファイルを生成するとともに、前記生成したバインディングライセンスを前記デバイス部に与える、請求項１に記載のデータ端末装置。

【請求項３】　前記ライセンスの取得時、
前記モジュール部は、前記記憶部から読出した前記暗号化機密ファイルを前記デバイス部から取得した前記バインディング鍵によって復号し、その復号した機密ファイルに前記取得したライセンスを機密情報として書込んで前記機密ファイルを更新し、その更新した機密ファイルを前記バインディング鍵によって暗号化し、その暗号化した暗号化機密ファイルを前記記憶部に更新記録し、前記書込んだライセンスを構成要素とする機密情報の管理番号を含むライセンス管理ファイルを作成して前記記憶部に書込む、請求項１に記載のデータ端末装置。

【請求項４】　前記ライセンスの送信時、
前記モジュール部は、前記デバイス部から取得した前記バインディング鍵によって前記記憶部から読出した前記暗号化機密ファイルを復号してライセンスを取得し、その取得したライセンスを外部へ出力する、請求項１に記載のデータ端末装置。

【請求項５】　前記ライセンスの出力時、
前記モジュール部は、前記ライセンスに対応し、かつ前記記憶部に記録された前記暗号化コンテンツデータと前記ライセンスとを外部へ出力する、請求項４に記載のデータ端末装置。

【請求項６】　前記デバイス部は、前記専用領域を指定する専用登録番号を前記モジュール部から受取り、その受取った専用登録番号によって前記バインディングライセンスを前記専用領域に格納する、請求項１に記載のデータ端末装置。

【請求項７】　前記ライセンスの出力時、
前記モジュール部は、前記専用登録番号を前記デバイス部へ送信することによって前記バインディング鍵を取得する、請求項６に記載のデータ端末装置。

【請求項８】　前記ライセンスの出力時、
前記モジュール部は、前記デバイス部に対する認証データを前記デバイス部へ送信し、前記デバイス部において前記認証データが認証された場合、前記バインディング鍵を取得する、請求項１から請求項７のいずれか１項に記載のデータ端末装置。

【請求項９】　前記ライセンスの出力時、
前記デバイス部は、前記バインディング鍵を暗号化して出力する、請求項１から請求項８のいずれか１項に記載のデータ端末装置。

【請求項１０】　前記ライセンスの出力時、
前記モジュール部は、前記取得したバインディング鍵によって前記暗号化機密ファイルを復号して機密ファイルを取得し、かつ、前記記憶部から読出したライセンス管理ファイルに含まれる機密情報の管理番号に一致する機密情報を前記取得した機密ファイルから読出すことによって外部へ出力するライセンスを取得する、請求項４に記載のデータ端末装置。

【請求項１１】　前記ライセンスの他のデータ端末装置への送信時、
前記モジュール部は、さらに、前記デバイス部において保持された公開暗号鍵を受取ることによって前記デバイス部はバインディングライセンスの書込みが可能であることを確認する、請求項１から請求項９のいずれか１項に記載のデータ端末装置。

【請求項１２】　前記暗号化コンテンツデータの他のデータ端末装置への移動時、
前記モジュール部は、前記ライセンスの複製ができないとき、前記他のデータ端末装置へ送信したライセンスを構成要素とする機密情報を削除し、その削除した機密情報の管理番号を削除してライセンス管理ファイルを更新し、もう１つのバインディング鍵を生成し、その生成したもう１つのバンディング鍵によって機密ファイルを暗号化して前記暗号化機密ファイルを更新する、請求項１０に記載のデータ端末装置。

【請求項１３】　前記暗号化コンテンツデータの他のデータ端末装置への移動時、
前記デバイス部は、前記もう１つのバインディング鍵を含むもう１つのバインディングライセンスを前記モジュール部から受け取り、その受取ったもう１つのバインディングライセンスを前記専用領域に上書きして格納する、請求項１１に記載のデータ端末装置。

【請求項１４】　前記ライセンスの他のデータ端末装置への送信時、
前記モジュール部は、前記他のデータ端末装置から受信した認証データを認証すると、ライセンスを他のデータ端末装置へ送信する、請求項１から請求項１２のいずれか１項に記載のデータ端末装置。
【請求項１５】　前記モジュール部は、前記ライセンスを暗号化した上で出力する、請求項１３に記載のデータ端末装置。
【請求項１６】　コンテンツデータを暗号化した暗号化コンテンツデータおよび前記暗号化コンテンツデータを復号して元の平文を得るためのライセンスを取得し、前記暗号化コンテンツデータおよび前記ライセンスを他のデータ端末装置へ出力するデータ端末装置であって、
前記暗号化コンテンツデータおよび前記ライセンスをソフトウエアによって取得するモジュール部と、
前記暗号化コンテンツデータと、ライセンス管理ファイルと、独自の暗号化を施した暗号化機密ファイルとを記憶する記憶部と、
バインディング鍵を含むバインディングライセンスを専用領域に格納するデバイス部とを備え、
前記暗号化機密ファイルを復号した機密ファイルは、前記デバイス部が格納するバインディングライセンスと同じバインディングライセンスを含み、
前記ライセンス管理ファイルは、前記暗号化コンテンツデータに対応し、かつ、前記ライセンスを構成要素とする機密情報に独自の暗号化を施した暗号化機密情報を含む、データ端末装置。
【請求項１７】　前記暗号化機密ファイルの初期化時、
前記モジュール部は、前記バインディング鍵を含めて前記バインディングライセンスを生成し、その生成したバインディングライセンスを格納した機密ファイルを生成し、その生成した機密ファイルに独自の暗号化を施して前記暗号化機密ファイルを生成するとともに、前記生成したバインディングライセンスを前記デバイス部に与える、請求項１６に記載のデータ端末装置。
【請求項１８】　前記ライセンスの取得時、
前記モジュール部は、前記ライセンスに独自の暗号化を施して暗号化機密情報を生成し、その暗号化機密情報を含むライセンス管理ファイルを生成して前記記憶部に書込む、請求項１６に記載のデータ端末装置。
【請求項１９】　前記ライセンスの送信時、
前記モジュール部は、前記デバイス部から取得した前記バインディング鍵が前記暗号化機密ファイルを復号して取得したバインディング鍵に一致すると、前記記憶部から読出した前記暗号化機密情報を復号してライセンスを取得し、その取得したライセンスと前記記憶部から読出した暗号化コンテンツデータとを他のデータ端末装置へ送信する、請求項１８に記載のデータ端末装置。
【請求項２０】　前記独自の暗号化方式は、データ端末装置から取得可能なデータ端末装置に固有の情報に関連付けた暗号化方式である、請求項１６に記載のデータ端末装置。
【請求項２１】　前記デバイス部は、前記専用領域を指定する専用登録番号を前記モジュール部から受取り、その受取った専用登録番号によって前記バインディングライセンスを前記専用領域に格納し、
前記モジュール部は、前記専用登録番号を含めて前記暗号化機密ファイルおよび前記ライセンス管理ファイルを生成する、請求項１６に記載のデータ端末装置。
【請求項２２】　前記ライセンスの送信時、
前記モジュール部は、前記専用登録番号を前記デバイス部へ送信することによって前記バインディング鍵を取得する、請求項２１に記載のデータ端末装置。
【請求項２３】　前記ライセンスの他のデータ端末装置への送信時、
前記モジュール部は、前記デバイス部に対する認証データを前記デバイス部へ送信し、前記デバイス部において前記認証データが認証された場合、前記バインディング鍵を取得する、請求項１６から請求項２３のいずれか１項に記載のデータ端末装置。
【請求項２４】　前記ライセンスの他のデータ端末装置への送信時、
前記モジュール部は、前記他のデータ端末装置から受信した認証データを認証すると、ライセンスを他のデータ端末装置へ送信する、請求項１６から請求項２３のいずれか１項に記載のデータ端末装置。
【請求項２５】　前記モジュール部は、配信サーバからインターネットによって前記暗号化コンテンツデータおよび前記ライセンスを取得する、請求項１から請求項２４のいずれか１項に記載のデータ端末装置。
【請求項２６】　記録媒体から平文のコンテンツデータを読出す媒体駆動部をさらに備え、
前記モジュール部は、前記媒体駆動部が読出したコンテンツデータに含まれる複製可否情報に基づいてライセンスを生成し、その生成したライセンスに含まれるライセンス鍵によって前記コンテンツデータを暗号化して暗号化コンテンツデータを生成することによって前記暗号化コンテンツデータおよび前記ライセンスを取得する、請求項１から請求項２４のいずれか１項に記載のデータ端末装置。
【請求項２７】　前記デバイス部は、さらに、配信サーバから前記暗号化コンテンツデータおよびライセンスを受信し、その受信したライセンスを保持し、
前記記憶部は、前記デバイス部によって受信された暗号化コンテンツデータを記憶する、請求項１から請求項２４のいずれか１項に記載のデータ端末装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は、コピーされた情

報に対する著作権保護を可能とするデータ配信システムにおいて用いられるデータ端末装置に関するものである。

【０００２】

【従来の技術】近年、インターネット等の情報通信網等の進歩により、再生端末等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

【０００３】このような情報通信網においては、デジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。

【０００４】したがって、このような情報通信網上において音楽データや画像データ等の著作者の権利が存在する創作物が伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

【０００５】一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介して著作物データの配信を行なうことができないとすると、基本的には、著作物データの複製に際し一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

【０００６】ここで、上述のようなデジタル情報通信網を介した配信ではなく、デジタルデータを記録した記録媒体を例にとって考えて見ると、通常販売されている音楽データを記録したＣＤ（コンパクトディスク）については、ＣＤから光磁気ディスク（ＭＤ等）への音楽データのコピーは、当該コピーした音楽を個人的な使用に止める限り原則的には自由に行なうことができる。ただし、デジタル録音等を行なう個人ユーザは、デジタル録音機器自体やＭＤ等の媒体の代金のうちの一定額を間接的に著作権者に対して著作権料として支払うことになっている。

【０００７】しかも、ＣＤからＭＤへデジタル信号である音楽データをコピーした場合、これらの情報がコピー劣化の殆どないデジタルデータであることに鑑み、記録可能なＭＤからさらに他のＭＤに音楽データとしてコピーすることは、著作権保護のために機器の構成上できないようになっている。

【０００８】このような事情からも、音楽データや画像データをデジタル情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。

【０００９】この場合、情報通信網を通じて公衆に送信される著作物である音楽データや画像データ等のコンテンツデータについて、一度受信されたコンテンツデータが、さらに勝手に複製されること、あるいは、複製できても利用されることを防止することが必要となる。

【００１０】そこで、コンテンツデータを暗号化した暗号化コンテンツデータを保持する配信サーバが、再生端末等の端末装置に装着されたメモリカードに対して端末装置を介して暗号化コンテンツデータを配信するデータ配信システムが提案されている。このデータ配信システムにおいては、予め認証局で認証されたメモリカードの公開暗号鍵とその証明書を暗号化コンテンツデータの配信要求の際に配信サーバへ送信し、配信サーバが認証された証明書を受信したことを確認した上でメモリカードに対して暗号化コンテンツデータと、暗号化コンテンツデータを復号するためのライセンス鍵を送信する。そして、暗号化コンテンツデータやライセンス鍵を配信する際、配信サーバおよびメモリカードは、配信毎に異なるセッションキーを発生させ、その発生させたセッションキーによって公開暗号鍵の暗号化を行ない、配信サーバ、メモリカード相互間で鍵の交換を行なう。

【００１１】最終的に、配信サーバは、メモリカード個々の公開暗号鍵によって暗号化され、さらにセッションキーによって暗号化したライセンスと、暗号化コンテンツデータをメモリカードに送信する。そして、メモリカードは、受信したライセンスと暗号化コンテンツデータをメモリカードに記録する。

【００１２】そして、メモリカードに記録した暗号化コンテンツデータを再生するときは、メモリカードを携帯電話機に装着する。携帯電話機は、通常の電話機能の他にメモリカードからの暗号化コンテンツデータを復号し、かつ、再生して外部へ出力するための専用回路も有する。

【００１３】このように、携帯電話機のユーザは、携帯電話機を用いて暗号化コンテンツデータを配信サーバから受信し、その暗号化コンテンツデータを再生することができる。

【００１４】一方、インターネットを用いて暗号化コンテンツデータをパーソナルコンピュータに配信することも行なわれている。そして、パーソナルコンピュータへの暗号化コンテンツデータとライセンスを同様な方法で配信することは可能ではあるが、パーソナルコンピュータにインストールされたソフトウェアによって暗号化コンテンツデータおよびライセンスの配信が受信され、ライセンスの保護が行なわれており、受信した暗号化コンテンツデータおよびライセンスを他のパーソナルコンピュータへ移動することは著作権保護の観点からラ行なわれていない。

【００１５】つまり、パーソナルコンピュータへ配信されたライセンスを記録したパーソナルコンピュータのＣＰＵに個別に付与された識別番号や起動プログラムであるＢＩＯＳの識別番号などの値に関連付けた暗号処理を用いて、そのまま他のパーソナルコンピュータにコピーしても、ライセンスを取り出せず、暗号化コンテンツ復

号して再生できない管理構造を採用している。そして、この管理下においてライセンスを他のパーソナルコンピュータへ移動できるサービスを提供したとすると、記録装置上で、ライセンスを特定することはできないものの、暗号化コンテンツデータおよびライセンスを管理し、記録している全てのデータのバックアップを取っておき、提供されたサービスによって、他のパーソナルコンピュータへ暗号化コンテンツデータおよびライセンスを移動させた後に、バックアップを取った暗号化コンテンツデータおよびライセンスを管理し、記録している全てのデータをパーソナルコンピュータへ戻せば移動前の状態を再現でき、暗号化コンテンツデータおよびライセンスを複製したのと同じことになる。このような管理においてのライセンスの移動は、セキュリティホールが明らかに存在する。したがって、ソフトウエアによってパーソナルコンピュータへ配信された暗号化コンテンツデータおよびライセンスを他のパーソナルコンピュータへ移動できないことになっている。

【００１６】

【発明が解決しようとする課題】しかし、パーソナルコンピュータに配信された暗号化コンテンツデータおよびライセンスをそのパーソナルコンピュータから、一切、取り出すことができないとすると、パーソナルコンピュータの破損や、バージョンアップによってＣＰＵが変動したときは、既に受信した暗号化コンテンツデータおよびライセンスを利用することができないという問題がある。

【００１７】そこで、本発明は、かかる問題を解決するためになされたものであり、その目的は、ソフトウエアによって配信された暗号化コンテンツデータおよびライセンスを他のデータ端末装置へ移動可能なデータ端末装置を提供することである。

【００１８】

【課題を解決するための手段および発明の効果】この発明によるデータ端末装置は、コンテンツデータを暗号化した暗号化コンテンツデータおよび暗号化コンテンツデータを復号して元の平文を得るためのライセンスを取得し、暗号化コンテンツデータおよびライセンスを他のデータ端末装置へ出力するデータ端末装置であって、暗号化コンテンツデータおよびライセンスをソフトウエアによって取得するモジュール部と、暗号化コンテンツデータと、ライセンス管理ファイルと、暗号化機密ファイルとを記憶する記憶部と、暗号化機密ファイルを復号し、かつ、その復号した機密ファイルを暗号化するバインディング鍵を含むバインディングライセンスを専用領域に格納するデバイス部とを備え、機密ファイルは、ライセンスを構成要素とする機密情報を含み、ライセンス管理ファイルは、暗号化コンテンツファイルに対応し、かつ、機密ファイルに含まれる機密情報の管理番号を含む。

【００１９】この発明によるデータ端末装置においては、モジュール部は、ソフトウェアによって暗号化コンテンツデータおよびライセンスを取得し、デバイス部から取出したバインディング鍵によって暗号化機密ファイルを復号し、取得したライセンスを復号した機密ファイルに書込み、バインディング鍵によって機密ファイルを暗号化して暗号化機密ファイルを生成する。つまり、モジュール部は、デバイス部においてハードウェアによって保持されるバインディング鍵を介して暗号化機密ファイルを開閉して取得したライセンスを管理する。

【００２０】したがって、この発明によれば、ソフトウェアによって取得された暗号化コンテンツデータを復号して再生するためのライセンスは、ハードウェアに保持されたバインディング鍵によって管理されるため、取得した暗号化コンテンツデータおよびライセンスを他のデータ端末装置へ移動できる。

【００２１】好ましくは、暗号化機密ファイルの初期化時、データ端末装置のモジュール部は、バインディング鍵を含めてバインディングライセンスを生成し、機密情報が空な機密ファイルを生成し、その生成した機密ファイルを生成したバインディング鍵によって暗号化して暗号化機密ファイルを生成するとともに、生成したバインディングライセンスをデバイス部に与える。

【００２２】暗号化機密ファイルの初期化時、モジュール部は、バインディング鍵を含むバインディングライセンスと空な機密ファイルとを生成し、機密ファイルをバインディング鍵によって暗号化を行なって暗号化機密ファイルを生成するとともにバインディングライセンスをデバイス部に保持する。

【００２３】したがって、この発明によれば、ソフトウェアによって取得した暗号化コンテンツデータのライセンスを格納する機密ファイルをソフト的に作成し、その作成した機密ファイルを管理するためのバインディングライセンスをハード的に管理できる。

【００２４】好ましくは、ライセンスの取得時、データ端末装置のモジュール部は、記憶部から読出した暗号化機密ファイルをデバイス部から取得したバインディング鍵によって復号し、その復号した機密ファイルに取得したライセンスを機密情報として書込んで機密ファイルを更新し、その更新した機密ファイルをバインディング鍵によって暗号化し、その暗号化した暗号化機密ファイルを記憶部に更新記録し、書込んだライセンスを構成要素とする機密情報の管理番号を含むライセンス管理ファイルを作成して記憶部に書込む。

【００２５】デバイス部から取得したバインディング鍵によって暗号化機密ファイルを開閉して取得したライセンスを機密ファイルに書込む。そして、その書込んだライセンスを構成要素とする機密情報の管理番号を含めてライセンス管理ファイルを作成する。

【００２６】したがって、この発明によれば、ソフト的

に取得した暗号化コンテンツデータのライセンスを管理番号によって管理できる。

【００２７】好ましくは、ライセンスの送信時、データ端末装置のモジュール部は、デバイス部から取得したバインディング鍵によって記憶部から読出した暗号化機密ファイルを復号してライセンスを取得し、その取得したライセンスを外部へ出力する。

【００２８】モジュール部は、デバイス部から取得したバインディング鍵によって暗号化機密ファイルを復号してライセンスを取得し、その取得したライセンスを外部へ出力する。

【００２９】したがって、この発明によれば、ソフト的に取得した暗号化コンテンツデータのライセンスをハード的に取得した暗号化コンテンツデータのライセンスと同じように他の装置へ移動できる。

【００３０】好ましくは、データ端末装置のモジュール部は、ライセンスの出力時、ライセンスに対応し、かつ記憶部に記録された暗号化コンテンツデータとライセンスとを外部へ出力する。

【００３１】ライセンスの外部への出力時、機密ファイルから取出したライセンスに対応する暗号化コンテンツデータを記憶部から読出し、暗号化コンテンツデータとライセンスとを外部へ出力する。

【００３２】したがって、この発明によれば、暗号化コンテンツデータおよびライセンスをソフト的に読出して他の装置へ暗号化コンテンツデータおよびライセンスを移動できる。

【００３３】好ましくは、データ端末装置のデバイス部は、専用領域を指定する専用登録番号をモジュール部から受取り、その受取った専用登録番号によってバインディングライセンスを専用領域に格納する。

【００３４】デバイス部は、専用登録番号を介して暗号化機密ファイルを開閉するためのバインディングライセンスを専用領域に格納する。

【００３５】したがって、この発明によれば、専用登録番号によってバインディングライセンスと暗号化コンテンツデータのライセンスとを対応付けることができる。

【００３６】好ましくは、ライセンスの出力時、データ端末装置のモジュール部は、専用登録番号をデバイス部へ送信することによってバインディング鍵を取得する。

【００３７】モジュール部は、専用登録番号を介して、記憶部から読出したいライセンスが格納された機密ファイルを開けるためのバインディング鍵を取得する。

【００３８】したがって、この発明によれば、専用登録番号によってバインディング鍵を正確に取得できる。

【００３９】好ましくは、ライセンスの出力時、データ端末装置のモジュール部は、デバイス部に対する認証データをデバイス部へ送信し、デバイス部において認証データが認証された場合、バインディング鍵を取得する。

【００４０】認証されたモジュール部のみにバインディング鍵が与えられる。したがって、この発明によれば、不正なバインディング鍵の流出を防止できる。

【００４１】好ましくは、ライセンスの出力時、データ端末装置のデバイス部は、バインディング鍵を暗号化して出力する。

【００４２】デバイス部は、ライセンスを管理するためのバインディング鍵を暗号化して出力する。

【００４３】したがって、この発明によれば、ライセンスを他の装置へ移動するとき、移動先でライセンスを管理するバインディング鍵を不正に取得されにくくできる。

【００４４】好ましくは、ライセンスの出力時、データ端末装置のモジュール部は、取得したバインディング鍵によって暗号化機密ファイルを復号して機密ファイルを取得し、かつ、記憶部から読出したライセンス管理ファイルに含まれる機密情報の管理番号に一致する機密情報を取得した機密ファイルから読出すことによって外部へ出力するライセンスを取得する。

【００４５】モジュール部は、デバイス部からバインディング鍵を取得して暗号化機密ファイルを復号し、その復号した機密ファイルに含まれる機密情報から管理番号に一致する機密情報を取得して外部へ出力しようとするライセンスを取得する。

【００４６】したがって、この発明によれば、管理番号を介して正確にライセンスを取得できる。

【００４７】好ましくは、ライセンスの他のデータ端末装置への送信時、データ端末装置のモジュール部は、さらに、デバイス部において保持された公開暗号鍵を受取ることによってデバイス部はバインディングライセンスの書込みが可能であることを確認する。

【００４８】モジュール部は、ライセンスの他の装置への送信時、デバイス部がバインディングライセンスの書込みが可能なデバイス部か否かをデバイス部から公開暗号鍵を受取ることによって確認する。

【００４９】したがって、この発明によれば、暗号化コンテンツデータのライセンスを移動した際、デバイス部に格納されたバインディングライセンスを書換えることによってライセンスを移動したことを認識可能である。

【００５０】好ましくは、暗号化コンテンツデータの他のデータ端末装置への移動時、データ端末装置のモジュール部は、ライセンスの複製ができないとき、他のデータ端末装置へ送信したライセンスを構成要素とする機密情報を削除し、その削除した機密情報の管理番号を削除してライセンス管理ファイルを更新し、もう１つのバインディング鍵を生成し、その生成したもう１つのバンディング鍵によって機密ファイルを暗号化して暗号化機密ファイルを更新する。

【００５１】移動したライセンスの複製が禁止されているとき、モジュール部は、移動したライセンスを削除するとともに、別のバインディング鍵を生成して暗号化機

密ファイルを更新する。

【００５２】したがって、この発明によれば、ライセンスが不正に複製されるのを防止できる。

【００５３】好ましくは、暗号化コンテンツデータの他のデータ端末装置への移動時、データ端末装置のデバイス部は、もう１つのバインディング鍵を含むもう１つのバインディングライセンスをモジュール部から受け取り、その受取ったもう１つのバインディングライセンスを専用領域に上書きして格納する。

【００５４】別のバインディング鍵が生成されたとき、デバイス部においてバインディングライセンスの書換えが行なわれる。

【００５５】したがって、この発明によれば、最新のバインディングライセンスによって暗号化コンテンツデータを再生するためのライセンスを管理できる。

【００５６】好ましくは、ライセンスの他のデータ端末装置への送信時、データ端末装置のモジュール部は、他のデータ端末装置から受信した認証データを認証すると、ライセンスを他のデータ端末装置へ送信する。

【００５７】モジュール部は、暗号化コンテンツデータのライセンスを移動しようとするデータ端末装置が正規の端末装置であることを確認してから暗号化コンテンツデータのライセンスを送信する。

【００５８】したがって、この発明によれば、正規なデータ端末装置間で暗号化コンテンツデータのライセンスを移動でき、暗号化コンテンツデータを十分に保護できる。

【００５９】好ましくは、データ端末装置のモジュール部は、ライセンスを暗号化した上で出力する。

【００６０】モジュール部は、ライセンスを暗号化した上で他のデータ端末装置へ移動する。

【００６１】したがって、この発明によれば、ライセンスの移動時に、そのライセンスを不正に取得されにくい。

【００６２】また、この発明によるデータ端末装置は、コンテンツデータを暗号化した暗号化コンテンツデータおよび暗号化コンテンツデータを復号して元の平文を得るためのライセンスを取得し、暗号化コンテンツデータおよびライセンスを他のデータ端末装置へ出力するデータ端末装置であって、暗号化コンテンツデータおよびライセンスをソフトウエアによって取得するモジュール部と、暗号化コンテンツデータと、ライセンス管理ファイルと、独自の暗号化を施した暗号化機密ファイルとを記憶する記憶部と、バインディング鍵を含むバインディングライセンスを専用領域に格納するデバイス部とを備え、暗号化機密ファイルを復号した機密ファイルは、デバイス部が格納するバインディングライセンスと同じバインディングライセンスを含み、ライセンス管理ファイルは、暗号化コンテンツデータに対応し、かつ、ライセンスを構成要素とする機密情報に独自の暗号化を施した暗号化機密情報を含む。

【００６３】この発明によるデータ端末装置においては、モジュール部は、ソフトウエアによって暗号化コンテンツデータおよびライセンスを取得し、その取得したライセンスに独自の暗号化を施して暗号化機密情報を生成し、その生成した暗号化機密情報を含むライセンス管理ファイルを作成して記憶部に書込む。また、ライセンスを管理するバインディングライセンスは機密ファイルに格納される。

【００６４】したがって、この発明によれば、ライセンスを管理するためのバインディング鍵はハードウエアによって保持されるため、ソフトウエアによって取得された暗号化コンテンツデータを復号して再生するためのライセンスを他のデータ端末装置へ移動できる。

【００６５】好ましくは、暗号化機密ファイルの初期化時、データ端末装置のモジュール部は、バインディング鍵を含めてバインディングライセンスを生成し、その生成したバインディングライセンスを格納した機密ファイルを生成し、その生成した機密ファイルに独自の暗号化を施して暗号化機密ファイルを生成するとともに、生成したバインディングライセンスをデバイス部に与える。

【００６６】モジュール部は、暗号化機密ファイルの初期化時、バインディング鍵を含むバインディングライセンスと空な機密ファイルとを生成し、機密ファイルに生成したバインディングライセンスを書込んで独自の暗号化を行なって暗号化機密ファイルを生成するとともにバインディングライセンスをデバイス部の専用領域に保持する。

【００６７】したがって、この発明によれば、ライセンスを管理するためのバインディング鍵はハードウエアによって保持されるため、ソフトウエアによって取得された暗号化コンテンツデータを復号して再生するためのライセンスを他のデータ端末装置へ移動できる。

【００６８】好ましくは、ライセンスの取得時、データ端末装置のモジュール部は、ライセンスに独自の暗号化を施して暗号化機密情報を生成し、その暗号化機密情報を含むライセンス管理ファイルを生成して記憶部に書込む。

【００６９】モジュール部は、取得したライセンスに独自の暗号化を施して記憶部で管理する。

【００７０】したがって、この発明によれば、ライセンスを独自の暗号化方式によって管理できる。

【００７１】好ましくは、ライセンスの送信時、データ端末装置のモジュール部は、デバイス部から取得したバインディング鍵が暗号化機密ファイルを復号して取得したバインディング鍵に一致すると、記憶部から読出した暗号化機密情報を復号してライセンスを取得し、その取得したライセンスと記憶部から読出した暗号化コンテンツデータとを他のデータ端末装置へ送信する。

【００７２】モジュール部は、デバイス部に格納された

バインディング鍵と記憶部に格納されたバインディング鍵とが一致する場合に限り、ライセンスを取得する。

【００７３】したがって、ハード的に管理されたバインディング鍵と同じバインディング鍵を有するモジュール部だけがライセンスを取得できる。

【００７４】好ましくは、独自の暗号化方式は、データ端末装置から取得可能なデータ端末装置に固有の情報に関連付けた暗号化方式である。

【００７５】モジュール部は、データ端末装置に固有な情報、たとえば、ＣＰＵのバージョン番号等に基づいた暗号化方式によってライセンスを暗号化する。

【００７６】したがって、この発明によれば、暗号化されたライセンスが他の装置へ不正に流出されても、そのライセンスが不正に取得されない。

【００７７】好ましくは、データ端末装置のデバイス部は、専用領域を指定する専用登録番号をモジュール部から受取り、その受取った専用登録番号によってバインディングライセンスを専用領域に格納し、モジュール部は、専用登録番号を含めて暗号化機密ファイルおよびライセンス管理ファイルを生成する。

【００７８】デバイス部は、モジュール部によって生成された専用登録番号によってバインディングライセンスをハード的に管理し、モジュール部は、生成した専用登録番号と取得したライセンスとを独自に暗号化してソフト的に管理する。

【００７９】したがって、この発明によれば、モジュール部は、専用登録番号を介してデバイス部に保持されたバインディング鍵を取得し、暗号化機密ファイルから読出したバインディング鍵とデバイス部から取得したバインディング鍵との一致を正確に判別できる。

【００８０】好ましくは、ライセンスの送信時、データ端末装置のモジュール部は、専用登録番号をデバイス部へ送信することによってバインディング鍵を取得する。

【００８１】モジュール部は、専用登録番号をデバイス部へ送信し、デバイス部は受信した専用登録番号によって指定された専用領域からバインディング鍵を取出して出力する。

【００８２】したがって、この発明によれば、専用登録番号によってバインディング鍵を正確に取得できる。

【００８３】好ましくは、ライセンスの他のデータ端末装置への送信時、データ端末装置のモジュール部は、デバイス部に対する認証データをデバイス部へ送信し、デバイス部において認証データが認証された場合、バインディング鍵を取得する。

【００８４】モジュール部のデバイス部に対する正当性が確認された場合だけ、モジュール部がバインディング鍵を取得する。

【００８５】したがって、この発明によれば、バインディング鍵の不正な取得を防止でき、その結果、ライセンスが他の端末装置へ不正に移動されることを防止できる。

【００８６】好ましくは、ライセンスの他のデータ端末装置への送信時、データ端末装置のモジュール部は、他のデータ端末装置から受信した認証データを認証すると、ライセンスを他のデータ端末装置へ送信する。

【００８７】暗号化コンテンツデータおよびライセンスを移動しようとするデータ端末装置が正規であることが確認されると、モジュール部は暗号化コンテンツデータおよびライセンスを他のデータ端末装置へ送信する。

【００８８】したがって、この発明によれば、正規のデータ端末装置間でのみ、暗号化コンテンツデータおよびライセンスの移動が可能である。

【００８９】好ましくは、データ端末装置のモジュール部は、配信サーバからインターネットによって暗号化コンテンツデータおよびライセンスを取得する。

【００９０】したがって、この発明によれば、各種のコンテンツデータを取得し、かつ、他の端末装置へ取得したコンテンツデータを移動できる。

【００９１】好ましくは、データ端末装置は、記録媒体から平文のコンテンツデータを読出す媒体駆動部をさらに備え、モジュール部は、媒体駆動部が読出したコンテンツデータに含まれる複製可否情報に基づいてライセンスを生成し、その生成したライセンスに含まれるライセンス鍵によってコンテンツデータを暗号化して暗号化コンテンツデータを生成することによって暗号化コンテンツデータおよびライセンスを取得する。

【００９２】データ端末装置は、リッピングによって暗号化コンテンツデータおよびライセンスを取得する。

【００９３】したがって、この発明によれば、通信手段以外の手段で頒布されるコンテンツデータも取得し、他のデータ端末装置へ移動できる。

【００９４】好ましくは、データ端末装置のデバイス部は、さらに、配信サーバから暗号化コンテンツデータおよびライセンスを受信し、その受信したライセンスを保持し、記憶部は、デバイス部によって受信された暗号化コンテンツデータを記憶する。

【００９５】デバイス部は、バインディングライセンスを保持するとともに、配信サーバから暗号化コンテンツデータおよびライセンスを受信し、その受信したライセンスをバインディングライセンスとともに保持する。

【００９６】したがって、この発明によれば、ハードウエアによって取得したライセンスとソフトウエアによって取得したライセンスとを殆ど同じセキュリティレベルで管理できる。

【００９７】

【発明の実施の形態】本発明の実施の形態について図面を参照しながら詳細に説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

【００９８】［実施の形態１］図１は、本発明によるデータ端末装置（パーソナルコンピュータ）が暗号化コン

テンツデータを取得するとともに、その取得した暗号化コンテンツデータを他のデータ端末装置（パーソナルコンピュータ）へ移動するデータ配信システムの全体構成を概念的に説明するための概略図である。

【００９９】なお、以下ではインターネットを介してデジタル音楽データを各パーソナルコンピュータのユーザに配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他の著作物としてのコンテンツデータ、たとえば画像データ、動画像データ等を配信する場合においても適用することが可能なものである。

【０１００】図１を参照して、パーソナルコンピュータ５０は、モデム４０およびインターネット網３０を介して、各パーソナルコンピュータのユーザからの配信要求（配信リクエスト）を配信サーバ１０に送信する。著作権の存在する音楽データを管理する配信サーバ１０は、データ配信を求めてアクセスして来たパーソナルコンピュータのユーザが所有するパーソナルコンピュータ５０が正当な認証データを持つか否か、すなわち、正規のパーソナルコンピュータは充分なセキュリティレベルを備えたコンテンツ保護を行っているか否かの認証処理を行ない、正当なコンテンツ保護を行っているパーソナルコンピュータに対して所定の暗号方式により音楽データ（以下コンテンツデータとも呼ぶ）を暗号化した上で、このような暗号化コンテンツデータおよび暗号化コンテンツデータを再生するために必要な情報としてのライセンスをパーソナルコンピュータ５０に配信する。

【０１０１】この場合、パーソナルコンピュータ５０は、モデム４０およびインターネット網３０を介して異なるセキュリティレベルによって暗号化コンテンツデータおよびライセンスを配信サーバ１０から受信して、管理することができる。すなわち、パーソナルコンピュータ５０は、ハード的にコンテンツ点津保護を実現するライセンス管理デバイスと、ソフト的にコンテンツ保護を実現するライセンス管理モジュールとを内蔵している。ライセンス管理デバイスは、アプリケーションソフトの助けを得て、配信サーバ１０からインターネット網３０等を介して暗号化コンテンツデータおよびライセンスを受信する。このライセンス管理デバイスは、暗号化コンテンツデータを再生するためのライセンスを受信するための暗号通信路を、直接、配信サーバとの間で確立し、受信したライセンスをハード的に保持するものであり、セキュリティレベルが高いものである。また、ライセンス管理モジュールも、同様に、所定の手順に従った暗号通信路を配信サーバとの間で確立し、ライセンスを受信し、暗号化して保護した上で、ハードディスク（ＨＤＤと言う）にライセンスを記録する。ライセンス管理デバイスよりも低いセキュリティレベルで暗号化コンテンツデータおよびライセンスを受信し、管理するものである。いずれの場合においても、暗号化コンテンツデータはそのままＨＤＤに記録される。ライセンス管理デバイスおよびライセンス管理モジュールについては、後に詳細に説明する。

【０１０２】以後、セキュリティレベルおよびライセンスを区別するためにメモリカード１１０あるいはライセンス管理デバイスなどのハードウエアによって機密性を保つセキュリティレベルをレベル２と呼び、レベル２のセキュリティを要求して配信サーバから送信されるライセンスをレベル２ライセンスと呼ぶこととする。同様に、ライセンス管理モジュールのようなソフトウエアによって機密性を保つセキュリティレベルをレベル１と呼び、レベル１のセキュリティレベルを要求して配信サーバから送信されるライセンスをレベル１ライセンスと呼ぶこととする。

【０１０３】さらに、図１においては、パーソナルコンピュータ５０は、ライセンス管理モジュールを使って音楽データを記録した音楽ＣＤ（Ｃｏｍｐａｃｔ　Ｄｉｓｋ）６０から取得した音楽データから、個人使用に限定したローカル使用に限定された暗号化コンテンツデータと、暗号化コンテンツデータを再生するためのライセンスとを生成することができる。この処理をリッピングと呼び、音楽ＣＤから暗号化コンテンツデータとライセンスとを取得する行為に相当する。リッピングによるローカル使用のライセンスは、その性格上、セキュリティレベルは決して高くないので、リッピングが如何なる手段でなされようともレベル１ライセンスとして扱われるもとする。リッピングの詳細については後述する。

【０１０４】またさらに、パーソナルコンピュータ５０は、ＵＳＢ（ＵｎｉｖｅｒｓａｌＳｅｒｉａｌ　Ｂｕｓ）ケーブル７０によって再生端末１００と接続し、配信サーバ１０から受信した暗号化コンテンツデータおよびライセンスを再生端末１００に装着されたメモリカード１１０に送信することが可能である。

【０１０５】またさらに、パーソナルコンピュータ５０は、受信した暗号化コンテンツデータおよびライセンスを通信ケーブル９０を介して、パーソナルコンピュータ８０へ送信する。

【０１０６】したがって、図１に示すデータ配信システムにおいては、パーソナルコンピュータ５０は、モデム４０およびインターネット網３０を介して配信サーバ１０から暗号化コンテンツデータとライセンスとを受信するとともに、音楽ＣＤから暗号化コンテンツデータとライセンスとを取得する。また、再生端末１００に装着されたメモリカード１１０は、パーソナルコンピュータ５０が配信サーバ１０または音楽ＣＤ６０から取得した暗号化コンテンツデータおよびライセンスを受信する。再生端末１００のユーザは、パーソナルコンピュータ５０を介することによって音楽ＣＤから暗号化コンテンツデータおよびライセンスを取得することが可能となる。

【0107】図1においては、たとえば携帯電話ユーザの再生端末100Cには、着脱可能なメモリカード110が装着される構成となっている。メモリカード110は、再生端末100により受信された暗号化コンテンツデータを受取り、上記配信にあたって行なわれた暗号化を復号した上で、再生端末100中の音楽再生部（図示せず）に与える。

【0108】さらに、たとえば携帯電話ユーザは、再生端末100に接続したヘッドホーン130等を介してこのようなコンテンツデータを「再生」して、聴取することが可能である。

【0109】また、図1においては、パーソナルコンピュータ50は、ライセンス管理モジュールを使って、ライセンス管理モジュールが直接管理するレベル1ライセンスを持つ暗号化コンテンツデータに限り、ライセンス管理モジュールと密接な連携を取る音楽再生プログラムを用いて再生する機能を備えることができる。レベル2ライセンスを持つ暗号化コンテンツデータの再生は、再生端末と同様な構成を持つハードウエアによって機密性を持つコンテンツ再生回路をパーソナルコンピュータに備えれば可能となる。パーソナルコンピュータにおける再生についての詳細な説明は、本出願における説明を簡略化するために省略する。

【0110】このような構成とすることで、充分なセキュリティレベルのコンテンツ保護機能をもつ、正規なライセンス管理デバイスあるいはライセンス管理モジュールを備えたパーソナルコンピュータでないと、配信サーバ10からコンテンツデータの配信を受信し、パーソナルコンピュータ30や再生端末100へ暗号化コンテンツデータを送信することが困難な構成となる。

【0111】しかも、配信サーバ10において、たとえば1曲分のコンテンツデータを配信するたびにその度数を計数しておくことで、パーソナルコンピュータのユーザがコンテンツデータを受信（ダウンロード）するたびに発生する著作権料を、インターネット網の使用料とともに徴収することとすれば、著作権者が著作権料を確保することが容易となる。

【0112】なお、図1において、再生端末100は、配信サーバ10と直接通信する機能を有しない再生端末を想定している。

【0113】図1に示したような構成においては、暗号化して配信されるコンテンツデータをパーソナルコンピュータのユーザ側で再生可能とするためにシステム上必要とされるのは、第1には、通信における暗号鍵を配信するための方式であり、さらに第2には、配信したいコンテンツデータを暗号化する方式そのものであり、さらに、第3には、このように配信されたコンテンツデータの無断コピーを防止するためのコンテンツデータ保護を実現する構成である。

【0114】本発明の実施の形態においては、特に、配信、移動、チェックアウト、チェックイン、および再生の各セッションの発生時において、これらのコンテンツデータの移動先に対する認証およびチェック機能を充実させ、非認証もしくは復号鍵の破られた記録装置およびデータ再生端末（コンテンツを再生できるデータ再生端末を再生端末またはパーソナルコンピュータとも言う。以下同じ））に対するコンテンツデータの出力を防止することによってコンテンツデータの著作権保護を強化する構成を説明する。

【0115】なお、以下の説明においては、配信サーバ10から、各パーソナルコンピュータ等にコンテンツデータを伝送する処理を「配信」と称することとする。

【0116】図2は、図1に示したデータ配信システムにおいて、使用される通信のためのデータ、情報等の特性を説明する図である。

【0117】まず、配信サーバ10より配信されるデータについて説明する。Dcは、音楽データ等のコンテンツデータである。コンテンツデータDcは、ライセンス鍵Kcで復号可能な暗号化が施される。ライセンス鍵Kcによって復号可能な暗号化が施された暗号化コンテンツデータ{Dc}Kcがこの形式で配信サーバ10よりパーソナルコンピュータのユーザに配布される。

【0118】なお、以下においては、{Y}Xという表記は、データYを、復号鍵Xにより復号可能な暗号化を施したことを示すものとする。

【0119】さらに、配信サーバ10からは、暗号化コンテンツデータとともに、コンテンツデータに関する著作権あるいはサーバアクセス関連等の平文情報としての付加情報Dc－infが配布される。また、ライセンスとして、ライセンス鍵Kc、配信サーバ10からのライセンス鍵等の配信を特定するための管理コードであるトランザクションIDが配信サーバ10とパーソナルコンピュータ50との間でやり取りされる。また、配信によらないライセンス、すなわち、個人使用を目的としたローカルでの使用のライセンスを特定するためにもトランザクションIDは使用される。配信によるものと、ローカル使用のものを区別するために、トランザクションIDの先頭は“0”で始まるものがローカル使用のトランザクションIDであり、“0”以外から始まるのものを配信によるトランザクションIDであるとする。さらに、ライセンスとしては、コンテンツデータDcを識別するためのコードであるコンテンツID、利用者側からの指定によって決定されるライセンス数や機能限定等の情報を含んだライセンス購入条件ACに基づいて生成される、記録装置（メモリカード、またはライセンス管理デバイス）におけるライセンスのアクセスに対する制限に関する情報であるアクセス制御情報ACmおよびデータ再生端末における制御情報である再生制御情報ACp等が存在する。具体的には、アクセス制限情報ACmはメモリカード、ライセンス管理モジュールおよびライセ

ンス管理モジュールからのライセンスまたはライセンス鍵を外部に出力に対するにあった手の制御情報であり、再生可能回数（再生のためにライセンス鍵を出力する数）、ライセンスの移動・複製に関する制限情報およびライセンスのセキュリティレベルなどがある。再生制御情報ＡＣｐは、再生するためにコンテンツ再生回路がライセンス鍵を受取った後に、再生を制限する情報であり、再生期限、再生速度変更制限、再生範囲指定（部分ライセンス）などがある。

【０１２０】本発明の実施の形態においては、簡単化のためアクセス制限情報ＡＣｍは再生回数の制限を行なう制御情報である再生回数〈０：再生不可、１～２５４：再生可能回数、２５５：制限無し）、ライセンスの移動および複製を制限する移動複製フラグ〈０：移動複製禁止・１：移動のみ可・２：移動複製可）、セキュリティレベル「１：レベル１、２：レベル２」の３項目とし、再生制御情報ＡＣｐは再生可能な期限を規定する制御情報である再生期限「ＵＴＣｔｉｍｅコード」のみを制限するものとする。ゆえに、以降では、再生制御情報ＡＣｐを再生期限ＡＣｐとも称する。

【０１２１】さらに、以後、トランザクションＩＤとコンテンツＩＤとを併せてライセンスＩＤと総称し、ライセンス鍵ＫｃとライセンスＩＤとアクセス制限情報ＡＣｍと再生期限ＡＣｐとを併せて、ライセンスと総称することとする。

【０１２２】本発明の実施の形態においては、記録装置（メモリカード、ライセンス管理デバイスおよびライセンス管理モジュール）やコンテンツデータを再生する再生端末のクラスごとに、コンテンツデータの配信、および再生を禁止することができるように禁止クラスリストＣＲＬ（Ｃｌａｓｓ　Ｒｅｖｏｃａｔｉｏｎ　Ｌｉｓｔ）の運用を行なう。以下では、必要に応じて記号ＣＲＬによって禁止クラスリスト内のデータを表わすこともある。

【０１２３】禁止クラスリスト関連情報には、ライセンスの配信、移動、チェックアウト、および再生が禁止される再生端末、メモリカード、ライセンス管理モジュール、およびライセンス管理デバイスのクラスをリストアップした禁止クラスリストデータＣＲＬが含まれる。コンテンツデータ保護に関わるライセンスの管理・蓄積およびライセンスを受けて再生を行なう全ての機器およびプログラムがリストアップの対象となる。

【０１２４】禁止クラスリストデータＣＲＬは、配信サーバ１０内で管理されるとともに、メモリカードや、ライセンス管理モジュールによってパーソナルコンピュータ５０内のハードディスク（ＨＤＤ）またはライセンス管理デバイス内にも記録保持される。このような禁止クラスリストは、随時バージョンアップしデータを更新していく必要があるが、データの変更については、基本的には暗号化コンテンツデータおよび／またはライセンス鍵等のライセンスを配信する際に、パーソナルコンピュータ（ライセンス管理デバイスまたはライセンス管理モジュール）から受取った禁止クラスリストの更新日時を判断し、更新されていないと判断されたとき、更新された禁止クラスリストをパーソナルコンピュータに配信する。また、ライセンス管理モジュール、ライセンス管理デバイス、および再生端末１００の間でも禁止クラスリストはやり取りされ、そのデータ変更も上述したのと同じである。さらに、禁止クラスリストの変更については、変更点のみを反映した差分データＣＲＬを配信サーバ１０側より発生して、これに応じてメモリカード、ハードディスク、およびライセンス管理デバイス内の禁止クラスリストＣＲＬに追加する構成とすることも可能である。また、禁止クラスリストの更新日時ＣＲＬｄａｔｅについては、メモリカード、ハードディスク、およびライセンス管理デバイス内に記録された禁止クラスリストＣＲＬ内に記録されていて、これを配信サーバ１０側で確認することによってバージョン管理を実行する。差分データＣＲＬ更新日時ＣＲＬｄａｔｅも含まれる。

【０１２５】このように、禁止クラスリストＣＲＬを、配信サーバのみならずメモリカードまたはパーソナルコンピュータ内においても保持運用することによって、クラス固有すなわち、再生端末およびメモリカードまたはパーソナルコンピュータ（ライセンス管理デバイスまたはライセンス管理モジュール）の種類に固有の復号鍵が破られた、再生端末およびメモリカードまたはパーソナルコンピュータへのライセンス鍵の供給を禁止する。このため、再生端末ではコンテンツデータの再生が、メモリカード、ライセンス管理モジュール、およびライセンス管理デバイスでは新たなライセンスを受信することができなくなる。

【０１２６】このように、メモリカードまたはライセンス管理デバイス内の、あるいはライセンス管理モジュールが管理するＨＤＤ内の禁止クラスリストＣＲＬは配信時に逐次データを更新する構成とする。また、メモリカード、ライセンス管理モジュール、およびライセンス管理デバイスにおける禁止クラスリストＣＲＬの管理は、上位レベルとは独立にメモリカード、ライセンス管理デバイス、およびライセンス管理モジュールによって制御されるハードディスクでタンパーレジスタントモジュール（Ｔａｍｐｅｒ　Ｒｅｓｉｓｔａｎｔ　Ｍｏｄｕｌｅ）に記録する。メモリカードまたはライセンス管理デバイス内では、ライセンスと同様に、ハード的に機密性を保証する高いレベルのタンパレジストモジュールによって記録され、ライセンス管理モジュールが管理するＨＤＤ内に記録された禁止クラスリストＣＲＬの管理は、暗号処理によって少なくとも改ざん防止処置が行われてパーソナルコンピュータのＨＤＤ等に記録される。言いかえれば、ソフトウエアによってその機密性が保証された低いレベルのタンパーレジスタントジュールによって

記録される。いずれにしても、ファイルシステムやアプリケーションプログラム等によって上位レベルから禁止クラスリストデータＣＲＬを改ざんすることが不可能な構成とする。この結果、データに関する著作権保護をより強固なものとすることができる。

【０１２７】図３は、図１に示すデータ配信システムにおいて使用される認証のためのデータ、情報等の特性を説明する図である。

【０１２８】再生端末、メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールには固有の公開暗号鍵ＫＰｐｙおよびＫＰｍｗがそれぞれ設けられ、公開暗号鍵ＫＰｐｙおよびＫＰｍｗは再生端末に固有の秘密復号鍵Ｋｐｙおよびメモリカード、ライセンス管理デバイス、およびライセンス管理モジュールに固有の秘密復号鍵Ｋｍｗによってそれぞれ復号可能である。これら公開暗号鍵および秘密復号鍵は、再生端末、メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールの種類ごとに異なる値を持つ。これらの公開暗号鍵および秘密復号鍵を総称してクラス鍵と称し、これらの公開暗号鍵をクラス公開暗号鍵、秘密復号鍵をクラス秘密復号鍵、クラス鍵を共有する単位をクラスと称する。クラスは、製造会社や製品の種類、製造時のロット等によって異なる。

【０１２９】また、コンテンツ再生デバイス（再生端末）のクラス証明書としてＣｐｙが設けられ、メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールのクラス証明書としてＣｍｗが設けられる。

【０１３０】これらのクラス証明書は、コンテンツ再生デバイス、メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールのクラスごとに異なる情報を有する。タンパーレジスタントモジュールが破られたり、クラス鍵による暗号が破られた、すなわち、クラス秘密復号鍵が取得されたクラス鍵に対しては、禁止クラスリストにリストアップされてライセンスの送信の禁止対象となる。

【０１３１】これらのコンテンツ再生デバイス、メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールに固有のクラス公開暗号鍵およびクラス証明書は、認証データ｛ＫＰｐｙ／／Ｃｐｙ｝ＫＰａの形式または認証データ｛ＫＰｍｗ／／Ｃｍｗ｝ＫＰａの形式で、出荷時にデータ再生デバイス（再生端末）、メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールにそれぞれ記録される。後ほど詳細に説明するが、ＫＰａは配信システム全体で共通の公開認証鍵である。

【０１３２】さらに、メモリカード１１０、ライセンス管理デバイス、およびライセンス管理モジュール内のデータ処理を管理するための鍵として、メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールという媒体または管理ソフトウエアごとに設定される公開暗号鍵ＫＰｍｃｘと、公開暗号鍵ＫＰｍｃｘで暗号化されたデータを復号することが可能なそれぞれに固有の秘密復号鍵Ｋｍｃｘが存在する。このメモリカード毎に子別な公開暗号鍵および秘密復号鍵を総称して個別鍵と称し、公開暗号鍵ＫＰｍｃｘを個別公開暗号鍵、秘密復号鍵Ｋｍｃｘを個別秘密復号鍵と称する。

【０１３３】メモリカード外とメモリカード間でのデータ授受、またはライセンス管理デバイス外とライセンス管理デバイス間でのデータ授受、またはライセンス管理モジュール外とライセンス管理モジュール間でのデータ授受における秘密保持のための暗号鍵として、コンテンツデータの配信、および再生が行なわれるごとに配信サーバ１０、再生端末１００、メモリカード１１０、ライセンス管理デバイス、ライセンス管理モジュールにおいて生成される共通鍵Ｋｓ１～Ｋｓ３が用いられる。

【０１３４】ここで、共通鍵Ｋｓ１～Ｋｓ３は、配信サーバ、再生端末もしくはメモリカードもしくはライセンス管理デバイスもしくはライセンス管理モジュール間の通信の単位あるいはアクセスの単位である「セッション」ごとに発生する固有の共通鍵であり、以下においてはこれらの共通鍵Ｋｓ１～Ｋｓ３を「セッションキー」とも呼ぶこととする。

【０１３５】これらのセッションキーＫｓ１～Ｋｓ３は、各セッションごとに固有の値を有することにより、配信サーバ、再生端末、メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールによって管理される。具体的には、セッションキーＫｓ１は、配信サーバによって配信セッションごとに発生される。セッションキーＫｓ２は、メモリカード、ライセンス管理デバイス、ライセンス管理モジュールによって配信セッションおよび再生セッションごとに発生し、セッションキーＫｓ３は、再生端末において再生セッションごとに発生される。各セッションにおいて、これらのセッションキーを授受し、他の機器で生成されたセッションキーを受けて、このセッションキーによる暗号化を実行したうえでライセンス鍵等の送信を行なうことによって、セッションにおけるセキュリティ強度を向上させることができる。

【０１３６】図４は、ソフトウエア（ライセンス管理モジュール）によって取得した暗号化コンテンツデータおよびライセンスを他のパーソナルコンピュータへ移動可能とするためにライセンス管理デバイスに関連付けて暗号化し管理するために必要なバインディングライセンスと、ソフトウエアによって取得した暗号化コンテンツデータおよびライセンスをメモリカード１１０へ貸出すチェックアウトセッションにおけるチェックアウト管理情報とを示したものである。

【０１３７】バインディングライセンスは、暗号化コンテンツデータを再生するためのレベル１ライセンスと、ライセンスのチェックアウトに関する情報を暗号化し

て、ソフトタンパレジスタントモジュールを実現するための共通鍵であるバインディング鍵と、バインディングライセンスに対する制御情報であるＡＣｍｂ，ＡＣｐｂと、バインディングライセンス用のトランザクションＩＤであるトランザクションＩＤｂと、バインディングＩＤ用のダミーであるコンテンツＩＤｂと、トランザクションＩＤｂとコンテンツＩＤｂとの総称であるバインディングＩＤとから成る。すなわち、ライセンス管理デバイスにライセンスとして記録することを前提としているため、ライセンスと同じ構成を持つ。

【０１３８】バインディング鍵Ｋｂは、ソフトウエアによって取得された暗号化コンテンツデータのライセンスを管理するものであり、ハードウエアによって保持される。そして、ハードウエアによって保持されたバインディング鍵Ｋｂによらなければライセンスを取出すことができないものである。また、制御情報ＡＣｍｂ，ＡＣｐｂは、暗号化コンテンツデータを再生するライセンスに含まれるＡＣｍ，ＡＣｐに相当するもので、固定値を持つ。ＡＣｍｂは、ライセンスの再生回数制限無し、移動複製禁止、かつ、セキュリティレベル１を表し、ＡＣｐｂは、再生期限が無期限であることを表す。

【０１３９】チェックアウト管理情報は、チェックアウト可能数と、チェックアウト先個別ＩＤと、チェックアウト時トランザクションＩＤとから成る。チェックアウト可能数は、暗号化コンテンツデータを貸出すことができる回数を示すものであり、暗号化コンテンツデータをチェックアウトする毎に数値が１づつ減じられ、暗号化コンテンツデータをチェックインする毎に数値が１づつ増加されるものである。また、チェックアウト先個別ＩＤは、暗号化コンテンツデータをチェックアウトするメモリカードを特定する識別情報であり、メモリカードが保持する個別公開暗号鍵ＫＰｍｃｘが該当する。チェックアウト時トランザクションＩＤは、チェックアウトするときに用いられるローカル使用のトランザクションＩＤである。

【０１４０】図５は、図１に示した配信サーバ１０の構成を示す概略ブロック図である。配信サーバ１０は、コンテンツデータを所定の方式に従って暗号化したデータや、コンテンツＩＤ等の配信情報を保持するための情報データベース３０４と、パーソナルコンピュータの各ユーザごとにコンテンツデータへのアクセス開始に従った課金情報を保持するための課金データベース３０２と、禁止クラスリストＣＲＬを管理するＣＲＬデータベース３０６と、情報データベース３０４に保持されたコンテンツデータのメニューを保持するメニューデータベース３０７と、ライセンスの配信ごとにコンテンツデータおよびライセンス鍵等の配信を特定するトランザクションＩＤの配信に関する記録して、保持する配信記録データベース３０８と、情報データベース３０４、課金データベース３０２、ＣＲＬデータベース３０６、メニューデータベース３０７、および配信記録データベース３０８からのデータをバスＢＳ１を介して受取り、所定の処理を行なうためのデータ処理部３１０と、通信網を介して、配信キャリア２０とデータ処理部３１０との間でデータ授受を行なうための通信装置３５０とを備える。

【０１４１】データ処理部３１０は、バスＢＳ１上のデータに応じて、データ処理部３１０の動作を制御するための配信制御部３１５と、配信制御部３１５に制御されて、配信セッション時にセッションキーＫｓ１を発生するためのセッションキー発生部３１６と、ライセンス管理デバイス、およびライセンス管理モジュールから送られてきた認証のための認証データ｛ＫＰｍｗ／／Ｃｍｗ｝ＫＰａを復号するための公開認証鍵ＫＰａを保持する認証鍵保持部３１３と、ライセンス管理デバイス、およびライセンス管理モジュールから送られてきた認証のための認証データ｛ＫＰｍｗ／／Ｃｍｗ｝ＫＰａを通信装置３５０およびバスＢＳ１を介して受けて、認証鍵保持部３１３からの公開認証鍵ＫＰａによって復号処理を行なう復号処理部３１２と、セッションキー発生部３１６より生成されたセッションキーＫｓ１を復号処理部３１２によって得られたクラス公開暗号鍵ＫＰｍｗを用いて暗号化して、バスＢＳ１に出力するための暗号化処理部３１８と、セッションキーＫｓ１によって暗号化された上で送信されたデータをバスＢＳ１より受けて、復号処理を行なう復号処理部３２０とを含む。

【０１４２】データ処理部３１０は、さらに、配信制御部３１５から与えられるライセンス鍵Ｋｃおよびアクセス制限情報ＡＣｍを、復号処理部３２０によって得られたメモリカード、ライセンス管理デバイス、およびライセンス管理モジュールの個別公開暗号鍵ＫＰｍｃｘによって暗号化するための暗号化処理部３２６と、暗号化処理部３２６の出力を、復号処理部３２０から与えられるセッションキーＫｓ２によってさらに暗号化してバスＢＳ１に出力するための暗号化処理部３２８とを含む。

【０１４３】配信サーバが保持する認証鍵は、配信サーバが配信しようとするライセンスの要求する受信側のセキュリティレベルによって異なる。セキュリティレベル２を要求するレベル２ライセンスを配信する配信サーバにあっては、セキュリティレベルがレベル２の機器が送信してくる認証データに対して認証処理が可能な認証鍵ＫＰａ２を保持する。また、配信しようとするライセンスがセキュリティレベル１を要求するレベル１ライセンスを配信する配信サーバにあっては、セキュリティレベルがレベル２の機器およびセキュリティレベルがレベル１の機器のいずれに対しても配信可能であるため、レベル２およびレベル１のそれぞれに対応した認証鍵ＫＰａ２およびＫＰａ１を保持し、相手のレベルに応じて使い分けることになる。さらには、送信された認証データが必要とする認証鍵は、クラス証明書Ｃｍｗの認証データとして暗号化されても、なお、平文として維持される領

域に記載され配信サーバ１０の配信制御部３１５が、復号処理部３１２にて復号前に容易に認証鍵を特定できる構成となっている。２つの認証鍵を区別するためにレベル２に対応した認証鍵ＫＰａ２をレベル２認証鍵ＫＰａ２、レベル１に対応した認証鍵ＫＰａ１を、レベル１認証鍵ＫＰａ１と称し、総じて認証鍵ＫＰａと称する。

【０１４４】配信サーバ１０の配信セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【０１４５】図６は、図１に示したパーソナルコンピュータ５０の構成を説明するための概略ブロック図である。パーソナルコンピュータ５０は、パーソナルコンピュータ５０の各部のデータ授受を行なうためのバスＢＳ２と、パーソナルコンピュータ内を制御すると共に、各種のプログラムを実行するためのコントローラ（ＣＰＵ）５１０と、データバスＢＳ２と、データバスＢＳ２に接続され、プログラムやデータを記録し、蓄積しておくための大容量記録装置であるハードディスク（ＨＤＤ）５３０およびＣＤ－ＲＯＭドライブ５４０と、ユーザからの指示を入力するためのキーボード５６０と、各種の情報を視覚的にユーザに与えるためのディスプレイ５７０とを含む。

【０１４６】パーソナルコンピュータ５０は、さらに、暗号化コンテンツデータおよびライセンスを再生端末１００等に通信する際にコントローラ５１０と端子５８０との間でデータの授受を制御するためのＵＳＢインタフェース５５０と、ＵＳＢケーブル７０を接続するための端子５８０と、配信サーバ１０とインタネット網３０およびモデム４０を介して通信する際にコントローラ５１０と端子５８５との間でデータの授受を制御するためのシリアルインタフェース５５５と、ケーブルによってモデム４０と接続するための端子５８５とを含む。

【０１４７】コントローラ５１０は、アプリケーションプログラムを実行することで、インターネット網３０を介してライセンス管理デバイス５２０またはライセンス管理モジュール５１１に暗号化コンテンツデータ等を配信サーバ１０から受信するために、配信サーバ１０との間でデータの授受を制御するとともに、ＣＤ－ＲＯＭドライブ５４０を介して音楽ＣＤからリッピングによって暗号化コンテンツデータおよびライセンスを取得する際の制御を行なう。

【０１４８】さらに、パーソナルコンピュータ５０は、配信サーバ１０からの暗号化コンテンツデータおよびライセンスの受信を行なう際に配信サーバ１０との間で各種の鍵のやり取りを行ない、配信された暗号化コンテンツデータを再生するためのライセンスをハード的に管理するライセンス管理デバイス５２０と、コントローラ５１０にて実行されるプログラムであって、配信サーバ１０からの暗号化コンテンツデータおよびレベル１ライセンスの受信をプログラムによって実行し、受信したライセンスに独自の暗号化を施した専用ライセンスを生成するコンテンツ管理モジュール５１１とを含む。

【０１４９】ライセンス管理デバイス５２０は、暗号化コンテンツデータおよびライセンスを配信サーバ１０から受信する際のデータの授受をハード的に行ない、受信したライセンスをハード的に管理するものであるため、高いセキュリティレベルを要求するレベル２のライセンスを扱うことが出る。一方、ライセンス管理モジュール５１１は、暗号化コンテンツデータおよびライセンスを配信サーバ１０から受信する際のデータの授受をコンロとローラ５１０にて実行されるプログラムを用いてソフト的に行ない、ライセンスの受信を、また、音楽ＣＤからリッピングによってローカル使用の暗号化コンテンツデータおよびライセンスの生成を行い、取得したライセンスに対して暗号処理などを施して保護し、ＨＤＤ５３０に蓄積して管理するものであるため、ライセンス管理デバイス５２０よりもセキュリティレベルが低い、レベル１ライセンスのみを扱う。なお、高いセキュリティレベルがレベル２である場合にはレベル１ライセンスも扱えることは言うまでもない。

【０１５０】このように、パーソナルコンピュータ５０は、配信サーバ１０からインターネット網３０を介して暗号化コンテンツデータおよびライセンスを受信するためのライセンス管理モジュール５１１およびライセンス管理デバイス５２０と、音楽ＣＤからリッピングによって暗号化コンテンツデータおよびライセンスを取得するためのＣＤ－ＲＯＭドライブ５４０とを内蔵するものである。

【０１５１】図7は、図１に示した再生端末１００の構成を説明するための概略ブロック図である。

【０１５２】再生端末１００は、再生端末１００の各部のデータ授受を行なうためのバスＢＳ３と、バスＢＳ３を介して再生端末１００の動作を制御するためのコントローラ１１０６と、外部からの指示を再生端末１００に与えるための操作パネル１１０８と、コントローラ１１０６等から出力される情報を携帯電話ユーザに視覚情報として与えるための表示パネル１１１０とを含む。

【０１５３】再生端末１００は、さらに、配信サーバ１０からのコンテンツデータ（音楽データ）を記憶しかつ復号化処理するための着脱可能なメモリカード１１０と、メモリカード１１０とバスＢＳ３との間のデータの授受を制御するためのメモリインタフェース１２００と、パーソナルコンピュータ５０から暗号化コンテンツデータおよびライセンスを受信する際にバスＢＳ３と端子１１１４との間のデータ授受を制御するためのＵＳＢインタフェース１１１２と、ＵＳＢケーブル７０を接続するための端子１１１４とを含む。

【０１５４】再生端末１００は、さらに、再生端末の種類（クラス）ごとにそれぞれ設定される、クラス公開暗号鍵ＫＰｐ１およびクラス証明書Ｃｐ１をクラス公開認

証鍵ＫＰａで復号することでその正当性を認証できる状態に暗号化した認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａ２を保持する認証データ保持部１５００を含む。ここで、再生端末１００のクラスｙは、ｙ＝１であるとする。また、再生端末は、ハード的に機密性を保持できるコンテンツ再生デバイスを用いて再生を提供する機器であるためセキュリティレベルはレベル２である。

【０１５５】再生端末１００は、さらに、再生端末（コンテンツ再生デバイス）のクラス秘密復号鍵であるＫｐ１を保持するＫｐ１保持部１５０２と、バスＢＳ３から受けたデータをＫｐ１によって復号しメモリカード１１０によって発生されたセッションキーＫｓ２を得る復号処理部１５０４とを含む。

【０１５６】再生端末１００は、さらに、メモリカード１１０に記憶されたコンテンツデータの再生を行なう再生セッションにおいてメモリカード１１０との間でバスＢＳ３上においてやり取りされるデータを暗号化するためのセッションキーＫｓ３を乱数等により発生するセッションキー発生部１５０８と、暗号化コンテンツデータの再生セッションにおいてメモリカード１１０からライセンス鍵Ｋｃおよび再生期限ＡＣｐを受取る際に、セッションキー発生部１５０８により発生されたセッションキーＫｓ３を復号処理部１５０４によって得られたセッションキーＫｓ２によって暗号化しバスＢＳ３に出力する暗号化処理部１５０６とを含む。

【０１５７】再生端末１００は、さらに、バスＢＳ３上のデータをセッションキーＫｓ３によって復号して、ライセンス鍵Ｋｃおよび再生期限ＡＣｐを出力する復号処理部１５１０と、バスＢＳ３より暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを受けて、復号処理部１５１０より取得したライセンス鍵Ｋｃによって復号しコンテンツデータを出力する復号処理部１５１６と、復号処理部１５１６の出力を受けてコンテンツデータを再生するための音楽再生部１５１８と、音楽再生部１５１８の出力をディジタル信号からアナログ信号に変換するＤＡ変換器１５１９と、ＤＡ変換器１５１９の出力をヘッドホーンなどの外部出力装置（図示省略）へ出力するための端子１５３０とを含む。

【０１５８】なお、図７においては、点線で囲んだ領域は暗号化コンテンツデータを復号して音楽データを再生するコンテンツ再生デバイス１５５０を構成する。また、図７においては、説明の簡素化のため、再生端末のうち本発明の音楽データの再生にかかわるブロックのみを記載し、再生端末が本来備えている通話機能に関するブロックについては、一部記載を省略している。

【０１５９】再生端末１００の各構成部分の各セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【０１６０】図８は、メモリカード１１０の構成を説明するための概略ブロック図である。既に説明したように、メモリカードに固有の公開暗号鍵および秘密復号鍵として、ＫＰｍｗおよびＫｍｗが設けられ、メモリカードのクラス証明書Ｃｍｗが設けられるが、メモリカード１１０においては、メモリカードのクラスを識別する自然数ｗ＝３で、メモリカードを識別する自然数ｘ＝４でそれぞれ表わされるものとする。また、メモリカード１１０は、ハード的に機密性を保持する機器であるためセキュリティレベルは２である。

【０１６１】したがって、メモリカード１１０は、認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａ２を保持する認証データ保持部１４００と、メモリカードごとに設定される固有の復号鍵である個別秘密復号鍵Ｋｍｃ４を保持するＫｍｃ保持部１４０２と、メモリカードの種類ごとに設定される固有のクラス秘密復号鍵Ｋｍ３を保持するＫｍ保持部１４２１と、個別秘密復号鍵Ｋｍｃ４によって復号可能な公開暗号鍵ＫＰｍｃ４を保持するＫＰｍｃ保持部１４１６とを含む。

【０１６２】このように、メモリカードという記録装置の暗号鍵を設けることによって、以下の説明で明らかになるように、配信されたコンテンツデータや暗号化されたライセンス鍵の管理をメモリカード単位で実行することが可能になる。

【０１６３】メモリカード１１０は、さらに、メモリインタフェース１２００との間で信号を端子１４２６を介して授受するインタフェース１４２４と、インタフェース１４２４との間で信号をやり取りするバスＢＳ４と、バスＢＳ４にインタフェース１４２４から与えられるデータから、メモリカードの種類ごとに固有のクラス秘密復号鍵Ｋｍ３をＫｍ保持部１４２１から受けて、配信サーバ１０が配信セッションにおいて生成したセッションキーＫｓ1を接点Ｐａに出力する復号処理部１４２２と、ＫＰａ保持部１４１４からレベル２認証鍵ＫＰａ２を受けて、バスＢＳ４に与えられるデータからレベル２認証鍵ＫＰａ２による復号処理を実行して復号結果と得られたクラス証明書をコントローラ１４２０に、得られたクラス公開鍵を暗号化処理部１４１０に出力する復号処理部１４０８と、切換スイッチ１４４２によって選択的に与えられる鍵によって、切換スイッチ１４４６によって選択的に与えられるデータを暗号化してバスＢＳ４に出力する暗号化処理部１４０６とを含む。

【０１６４】メモリカード１１０は、さらに、各セッションにおいてセッションキーＫｓ２を発生するセッションキー発生部１４１８と、セッションキー発生部１４１８の出力したセッションキーＫｓ２を復号処理部１４０８によって得られるクラス公開暗号鍵ＫＰｐｙもしくはＫＰｍｗによって暗号化してバスＢＳ４に送出する暗号化処理部１４１０と、バスＢＳ４よりセッションキーＫｓ２によって暗号化されたデータを受けてセッションキー発生部１４１８より得たセッションキーＫｓ２によって復号する復号処理部１４１２と、暗号化コンテンツデ

ータの再生セッションにおいてメモリ１４１５から読出されたライセンス鍵Ｋｃおよび再生期限ＡＣｐを、復号処理部１４１２で復号された他のメモリカード１１０に固有の個別公開暗号鍵ＫＰｍｃｘ（≠４）で暗号化する暗号処理部１４１７とを含む。

【０１６５】メモリカード１１０は、さらに、バスＢＳ４上のデータを個別公開暗号鍵ＫＰｍｃ４と対をなすメモリカード１１０固有の個別秘密復号鍵Ｋｍｃ４によって復号するための復号処理部１４０４と、禁止クラスリストデータＣＲＬと、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを再生するためのライセンス（Ｋｃ，ＡＣｐ，ＡＣｍ，ライセンスＩＤ）と、付加情報Ｄａｔａ－ｉｎｆと、暗号化コンテンツデータの再生リストファイルと、ライセンスを管理するためのライセンス管理ファイルとをバスＢＳ４より受けて格納するためのメモリ１４１５とを含む。メモリ１４１５は、例えば半導体メモリによって構成される。また、メモリ１５１５は、禁止クラスリストＣＲＬを記録するためのＣＲＬ領域１４１５Ａと、ライセンスを記録するライセンス領域１４１５Ｂと、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃ、暗号化コンテンツデータの関連情報Ｄｃ－ｉｎｆ、メモリカードに記録された暗号化コンテンツデータやライセンスをアクセスするための基本的な情報を記録する再生リストファイル、およびライセンスを管理するために必要な情報を暗号化コンテンツデータごとに記録するライセンス管理ファイルを記録する外部から直接アクセスが可能なデータ領域１４１５Ｃとから成る。ライセンス管理ファイルおよび再生リストファイルの詳細については後述する。

【０１６６】また、ライセンス領域１４１５Ｂは、ライセンス（コンテンツ鍵Ｋｃ、再生制御情報ＡＣｐ、アクセス制限情報ＡＣｍ、ライセンスＩＤ）を記録するためにエントリと呼ばれるライセンス専用の記録単位でライセンスを格納する。ライセンスに対してアクセスする場合には、ライセンスが格納されている、あるいは、ライセンスを記録したいエントリをエントリ番号によって指定する構成になっている。

【０１６７】メモリカード１１０は、さらに、バスＢＳ４を介して外部との間でデータ授受を行ない、バスＢＳ４との間で再生情報等を受けて、メモリカード１１０の動作を制御するためのコントローラ１４２０とを含む。

【０１６８】なお、データ領域１４１５Ｃを除く全ての構成は、耐タンパモジュール領域に構成される。

【０１６９】図９は、パーソナルコンピュータ５０に内蔵されたライセンス管理デバイス５２０の構成を示す概略ブロック図である。ライセンス管理デバイス５２０は、メモカード１１０におけるデータ領域１４１５Ｃに相当する領域を必要としない点、インタフェース１４２４の機能および端子１４２６の形状が異なるインタフェース５２２４と端子５２２６とを備える点が異なるのみで、基本的にメモリカード１１０と同じ構成から成る。ライセンス管理デバイス５２０の認証データ保持部５２００、Ｋｍｃ保持部５２０２、復号処理部５２０４、暗号処理部５２０６、復号処理部５２０８、暗号処理部５２１０、復号処理部５２１２、ＫＰａ保持部５２１４、ＫＰｍｃ保持部５２１６、暗号処理部５２１７、セッションキー発生部５２１８、コントローラ５２２０、Ｋｍ保持部５２２１、復号処理部５２２２、インタフェース５２２４、端子５２２６、切換スイッチ５２４２，５２４６は、それぞれ、メモリカード１１０の認証データ保持部１４００、Ｋｍｃ保持部１４０２、復号処理部１４０４、暗号処理部１４０６、復号処理部１４０８、暗号処理部１４１０、復号処理部１４１２、ＫＰａ保持部１４１４、ＫＰｍｃ保持部１４１６、暗号処理部１４１７、セッションキー発生部１４１８、コントローラ１４２０、Ｋｍ保持部１４２１、復号処理部１４２２、切換スイッチ１４４２，１４４６と同じである。ただし、認証データ保持部５２００は、認証データ｛ＫＰｍ７／／Ｃｍ７｝ＫＰａ２を保持し、ＫＰｍｃ保持部５２１６は、個別公開暗号鍵ＫＰｍ８を保持し、Ｋｍ保持部５２０２は、クラス秘密復号鍵Ｋｍ７を保持し、Ｋｍｃ保持部５２２１は、個別秘密復号鍵Ｋｍｃ８を保持する。ライセンス管理デバイス５２０のクラスを表す自然数ｗはｗ＝７であり、ライセンス管理デバイス５２０を識別するための自然数ｘはｘ＝８であるとする。

【０１７０】ライセンス管理デバイス５２０は、禁止クラスリストＣＲＬとライセンス（Ｋｃ，ＡＣｐ，ＡＣｍ，ライセンスＩＤ）とを記録するメモリ５２１５を、メモリカード１１０のメモリ１４１５に代えて含む。メモリ５２１５は、禁止クラスリストＣＲＬを記録したＣＲＬ領域５２１５Ａと、ライセンスを記録したライセンス領域５２１５Ｂとから成る。

【０１７１】さらに、ライセンス管理デバイス５２０は、ライセンス管理モジュール５１１が利用するバインディングライセンスを保持する必要がある。したがって、ＫＰａ保持部５２１４は、２つの認証鍵ＫＰａ２およびＫＰａ１を保持する。異なるレベルからの制御については、後ほどフローチャートを使用して詳細に説明する。

【０１７２】更に、ライセンス管理モジュール５１１はライセンスを管理するプログラムであり、セキュリティレベルは１である。また、ライセンス管理モジュール５１１は、ライセンス管理デバイス５２０とほぼ同一の構成を持つ管理プログラムなのでライセンス管理モジュール５１１のクラスを表す自然数ｗはｗ＝５であり、ライセンス管理デバイス５２０を識別するための自然数ｘはｘ＝６であるとする。したがって、ライセンス管理モジュール５１１は、認証データ｛ＫＰｍ５／／Ｃｍ５｝ＫＰａ１、個別公開暗号鍵ＫＰｍ６、クラス秘密復号鍵Ｋｍ５、個別秘密復号鍵Ｋｍｃ６を保持する。また、２つ

の認証鍵ＫＰａ2およびＫＰａ１を保持する。

【０１７３】以下、図１に示すデータ配信システムにおける各セッションの動作について説明する。

【０１７４】［初期化］パーソナルコンピュータ５０が配信サーバ１０から暗号化コンテンツデータおよびライセンスの配信を受ける前に行なわれる初期化について説明する。

【０１７５】図１０～図１２は、パーソナルコンピュータ５０が暗号化コンテンツデータおよびライセンスを配信サーバ１０から受信する前に行なわれる初期化を説明するための第１～第３のフローチャートである。

【０１７６】図１０を参照して、バイディングライセンスの生成がキーボード５６０を介してリクエストされると（ステップＳ１０）、ライセンス管理モジュール５１１は、バインディング鍵Ｋｂを生成し（ステップＳ１２）、次いで、トランザクションＩＤｂ、コンテンツＩＤｂ、所定の制御情報ＡＣｍｂおよびＡＣｐｂを生成する（ステップＳ１４）。ステップＳ１２，Ｓ１４はバインディングライセンスの生成処理である。

【０１７７】そして、ライセンス管理モジュール５１１は、ライセンス管理デバイス５２０に対してバスＢＳ２を介して認証データの出力を指示する（ステップＳ１６）。

【０１７８】そうすると、ライセンス管理デバイス５２０のコントローラ５２２０は、端子５２２６、インタフェース５２２４、およびバスＢＳ５を介して認証データの出力指示を受取り、認証データ保持部５２００からバスＢＳ５を介して認証データ｛ＫＰｍ７／／Ｃｍ７｝ＫＰａ２を取得し、バスＢＳ５、インタフェース５２２４および端子５２２６を介して認証データ｛ＫＰｍ７／／Ｃｍ７｝ＫＰａ２を出力する（ステップＳ１８）。ライセンス管理モジュール５１１は、バスＢＳ２を介して認証データ｛ＫＰｍ７／／Ｃｍ７｝ＫＰａ２を受信し（ステップＳ２０）、認証データ｛ＫＰｍ７／／Ｃｍ７｝ＫＰａをレベル２認証鍵ＫＰａ２によって復号する（ステップＳ２２）。

【０１７９】ライセンス管理モジュール５１１は、復号処理結果から、処理が正常に行なわれたか否か、すなわち、ライセンス管理デバイス５２０が正規のライセンス管デバイスからの公開暗号鍵ＫＰｍ７と証明書Ｃｍ７とを保持することを認証するために、正規の機関でその正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行なう（ステップＳ２４）。正当な認証データであると判断された場合、ライセンス管理モジュール５１１は、公開暗号鍵ＫＰｍ７および証明書Ｃｍ７を承認し、受理する。そして、次の処理（ステップＳ２６）へ移行する。正当な認証データでない場合には、非承認とし、公開暗号鍵ＫＰｍ７および証明書Ｃｍ７を受理しないで処理を終了する（ステップＳ６８）。

【０１８０】認証の結果、正規の機器であることが認識されると、ライセンス管理モジュール５１１は、次に、ライセンス管理デバイスのクラス証明書Ｃｍ７が禁止クラスリストＣＲＬにリストアップされているかどうかをハードディスク（ＨＤＤ）５３０に照会し、これらのクラス証明書が禁止クラスリストの対象になっている場合には、ここで初期化を終了する（ステップＳ６８）。

【０１８１】一方、ライセンス管理デバイス５２０のクラス証明書が禁止クラスリストの対象外である場合には次の処理に移行する（ステップＳ２６）。

【０１８２】認証の結果、正当な認証データを持つライセンス管理デバイスからのアクセスであり、クラスが禁止クラスリストの対象外であることが確認されると、ライセンス管理モジュール５１１は、セッションキーＫｓ２ａを生成する（ステップＳ２８）。

【０１８３】図１１を参照して、ライセンス管理モジュール５１１は、セッションキーＫｓ２ａをクラス公開暗号鍵ＫＰｍ７によって暗号化して暗号化データ｛Ｋｓ２ａ｝Ｋｍ７を生成し（ステップＳ３０）、暗号化データ｛Ｋｓ２ａ｝Ｋｍ７をバスＢＳ２を介してライセンス管理デバイス５２０へ出力する（ステップＳ３２）。ライセンス管理デバイス５２０のコントローラ５２２０は、端子５２２６、インタフェース５２２４、およびバスＢＳ５を介して暗号化データ｛Ｋｓ２ａ｝Ｋｍ７を受け、復号処理部５２２２は、Ｋｍ保持部５２２１から出力されるクラス秘密復号鍵Ｋｍ７によって暗号化データ｛Ｋｓ２ａ｝Ｋｍ７を復号してセッションキーＫｓ２ａを受理する（ステップＳ３４）。コントローラ５２２０は、セッションキーＫｓ２ａを受理したことに伴い、セッションキー発生部５２１８を制御してセッションキーＫｓ２ｂを発生させる。そうすると、セッションキー発生部５２１８は、セッションキーＫｓ２ｂを生成し（ステップＳ３６）、コントローラ５２２０は、バスＢＳ５を介してメモリ５２１５のＣＲＬ領域５２１５Ａから禁止クラスリストＣＲＬの更新日時ＣＲＬｄａｔｅを取得し、その取得した更新日時ＣＲＬｄａｔｅをバスＢＳ５を介して切換スイッチ５２４６へ出力する（ステップＳ３８）。そすすると、暗号処理部５２０６は、切換スイッチ５２４６を順次切換えることによって受取ったセッションキーＫｓ２ｂ、個別公開暗号鍵ＫＰｍｃ８および更新日時ＣＲＬｄａｔｅを復号処理部５２２２からのセッションキーＫｓ２ａによって暗号化する。コントローラ５２２０は、バスＢＳ５上の暗号化データ｛Ｋｓ２ｂ／／ＫＰｍｃ８／／ＣＲＬｄａｔｅ｝Ｋｓ２ａをインタフェース５２２４および端子５２２６を介して出力する（ステップＳ４０）。

【０１８４】ライセンス管理モジュール５１１は、バスＢＳ２を介して暗号化データ｛Ｋｓ２ｂ／／ＫＰｍｃ８／／ＣＲＬｄａｔｅ｝Ｋｓ２ａを受取り、暗号化データ｛Ｋｓ２ｂ／／ＫＰｍｃ８／／ＣＲＬｄａｔｅ｝Ｋｓ２

aをセッションキーKs2aによって復号してセッションキーKs2b、個別公開暗号鍵KPmc8、および更新日時CRLdateを受理する（ステップS42）。そして、ライセンス管理モジュール511は、ステップS12，S14で生成したバインディングライセンス（トランザクションIDb、コンテンツIDb、バインディング鍵Kb、および制御情報ACmb、ACpb）を公開暗号鍵KPmc8によって暗号化して暗号化データ{トランザクションIDb//コンテンツIDb//Kb//ACmb//ACpb}Kmc8を生成する（ステップS44）。

【0185】図12を参照して、ライセンス管理モジュール511において、ライセンス管理デバイス520から送信された禁止クラスリストの更新日時CRLdateがハードディスク（HDD）530に保持されている禁止クラスリストCRLの更新日時から、いずれが保持する禁止クラスリストが新しいかが比較される。ライセンス管理デバイス520の禁止クラスリストCRLの方が新しいとき、ステップS48へ移行する。また、逆に、ライセンス管理モジュール511の禁止クラスリストCRLの方が新しいときはステップS52へ移行する（ステップS46）。

【0186】ライセンス管理デバイス520の禁止クラスリストCRLの方が新しいと判断されたとき、ライセンス管理モジュール511は、暗号化データ{トランザクションIDb//コンテンツIDb//Kb//ACmb//ACpb}Kmc8をライセンス管理デバイス520において発生されたセッションキーKs2bによって暗号化を行い、暗号化データ{{トランザクションIDb//コンテンツIDb//Kb//ACmb//ACpb}Kmc8}Ks2bをバスBS2を介してライセンス管理デバイス520へ出力する（ステップS48）。

【0187】そして、ライセンス管理デバイス520のコントローラ5220は、暗号化データ{{トランザクションIDb//コンテンツIDb//Kb//ACmb//ACpb}Kmc8}Ks2bを端子5226およびインタフェース5224を介して受取り、セッションキー発生部5218によって発生されたセッションキーKs2bによって復号し、{トランザクションIDb//コンテンツIDb//Kc//ACmb//ACpb}Kmc8を受理する（ステップS50）。その後、ステップS60へ移行する。

【0188】一方、ライセンス管理モジュール511において、ライセンス管理モジュール511の禁止クラスリストCRLの方が新しいと判断されると、ライセンス管理モジュール511は、ライセンス管理デバイス520が保持する禁止クラスリストCRLを更新するため、バスBS2を介してHDD530から更新日時CRLdate以降の更新分を差分CRLとして取得する（ステップS52）。

【0189】そして、ライセンス管理モジュール511は、禁止クラスリストの差分CRLと暗号化データ{トランザクションIDb//コンテンツIDb//Kb//ACmb//ACpb}Kmc8とを、ライセンス管理デバイス520において生成されたセッションキーKs2bによって暗号化し、暗号化データ{CRLdate//{トランザクションIDb//コンテンツIDb//Kb//ACmb//ACpb}Kmc8}Ks2bをバスBS2を介してライセンス管理デバイス520へ出力する（ステップS54）。

【0190】ライセンス管理デバイス520のコントローラ5220は、端子5226およびインタフェース5224を介して、バスBS5に与えられた受信データを復号処理部5212によって復号する。復号処理部5212は、セッションキー発生部5218から与えられたセッションキーKs2bを用いてバスBS5の受信データを復号しバスBS5に出力する（ステップS56）。

【0191】この段階で、バスBS5には、Kmc保持部5221に保持される個別秘密復号鍵Kmc8で復号可能な{トランザクションIDb//コンテンツIDb//Kb//ACmb//ACpb}Kmc8と、差分CRLとが出力される（ステップS56）。コントローラ5220の指示によって受理した差分CRLによってメモリ5215内のCRL領域5215Aを差分CRLに基づいて更新する（ステップS58）。

【0192】ステップS48，S50は、送信側のライセンス管理モジュール511の禁止クラスリストCRLより、受信側のライセンス管理デバイス520の禁止クラスリストCRLが新しい場合のバインディング鍵Kb等のライセンス管理デバイス520への送信動作であり、ステップS52，S54，S56，S58は、受信側のライセンス管理デバイス520の禁止クラスリストCRLより、送信側のライセンス管理モジュール511の禁止クラスリストCRLが新しい場合のバインディング鍵Kb等のライセンス管理デバイス520への送信動作である。このように、ライセンス管理デバイス520から送られてきた禁止クラスリストの更新日時CRLdateを比較し、受信側の禁止クラスリストCRLが送信側の禁止クラスリストCRLより古いとき、禁止クラスリストの差分データである差分CRLをHDD530から取得し、差分CRLをライセンス管理デバイス520に配信することによって、常に新しい禁止クラスリストCRLを保持させるようにしている。

【0193】ステップS50またはステップS58の後、コントローラ5220の指示によって、暗号化データ{トランザクションIDb//コンテンツIDb//Kb//ACmb//ACpb}Kmc8は、復号処理部5204において、秘密復号鍵Kmc8によって復号され、バインディングライセンス（バインディング鍵K

ｂ、トランザクションＩＤｂ、コンテンツＩＤｂ、制御情報ＡＣｍＺ，ＡＣｐ）が受理される（ステップＳ６０）。

【０１９４】そして、ライセンス管理モジュール５１１は、バインディングライセンスを格納するためのエントリ番号「０」をライセンス管理デバイス５２０へ入力し（ステップＳ６２）、ライセンス管理デバイス５２０のコントローラ５２２０は、端子５２２６、インタフェース５２２４、およびバスＢＳ５を介してエントリー番号「０」を受取り、メモリ５２１５のライセンス領域５２１５Ｂのうち、受取ったエントリ番号「０」によって指定された領域にバイディングライセンス（トランザクションＩＤｂ、コンテンツＩＤｂ、バインディング鍵Ｋｂ、制御情報ＡＣｍｂ，ＡＣｐｂ）を格納する（ステップＳ６４）。

【０１９５】ライセンス管理モジュール５１１が、バインディング鍵Ｋｂを記録するためにライセンス管理デバイス５２０の領域を確認し、登録の準備を行なう図１０のステップ１６から図１１のステップ４２までの一連の処理を「デバイス確認処理」、バインディング鍵Ｋｂをライセンス管理デバイス５２０のライセンス領域５２１５Ｂに格納する図１１のステップＳ４４から図１２のステップＳ６４までの一連の処理を「バインディング鍵登録処理」と称する。

【０１９６】一方、ライセンス管理モジュール５１１は、機密情報（レベル１ライセンスおよびチェックアウト情報）が空な平文の機密ファイルを生成し、バインディング鍵Ｋｂによって機密ファイルを暗号化した暗号化機密ファイル１６０を生成して暗号化機密ファイル１６０をＨＤＤ５３０に記録し（ステップＳ６６）、初期化の動作を終了する（ステップＳ６８）。

【０１９７】このように、パーソナルコンピュータ５０のライセンス管理モジュール５１１は、初期化動作において、バインディングライセンスを生成し、ライセンス管理デバイス５２０におけるメモリ５２１５のライセンス領域５２１５Ｂのうち、エントリ番号「０」によって指定される領域に生成したバインディングライセンスを格納するとともに、生成したバインディングライセンスに含まれるバインディング鍵Ｋｂによって機密ファイルを暗号化した暗号化機密ファイル１６０を生成する。そして、この暗号化機密ファイル１６０は、ライセンス管理モジュール５１１によって配信サーバ１０から受信したライセンスを格納するためのものである。また、このようにバインディング鍵Ｋｂによって機密ファイルを暗号化することによりバインディング鍵Ｋｂがないと暗号化機密ファイル１６０からライセンスを取出すことができないため、バインディング鍵Ｋｂは暗号化コンテンツデータのライセンスを管理するための共通鍵である。そして、このバインディング鍵Ｋｂはライセンス管理デバイス５２０のメモリ５２１５に格納されているため、バインディング鍵Ｋｂをハードウエアによって管理することができる。その結果、バインディング鍵Ｋｂを介してＨＤＤ５３０に記録された暗号化機密ファイル１６０でソフト的に管理される暗号化コンテンツデータのライセンスをハードウエアによって管理することになる。したがって、後述するように、ソフトウエアによって受信された暗号化コンテンツデータおよびライセンスを他のパーソナルコンピュータ８０へ移動できる。

【０１９８】［配信１］次に、図１に示すデータ配信システムにおいて、配信サーバ１０からパーソナルコンピュータ５０のライセンス管理デバイス５２０へ暗号化コンテンツデータおよびセキュリティレベル２を要求するレベル２ライセンスを配信する動作について説明する。なお、この動作を「配信１」という。

【０１９９】図１３～図１６は、図１に示すデータ配信システムにおける暗号化コンテンツデータの購入時に発生するパーソナルコンピュータ５０に内蔵されたライセンス管理デバイス５２０への配信動作（以下、配信セッションともいう）を説明するための第１～第４のフローチャートである。

【０２００】図１３における処理以前に、パーソナルコンピュータ５０のユーザは、配信サーバ１０に対してモデム４０を介して接続し、購入を希望するコンテンツに対するコンテンツＩＤを取得していることを前提としている。

【０２０１】図１３を参照して、パーソナルコンピュータ５０のユーザからキーボード５６０を介してコンテンツＩＤの指定による配信リクエストがなされる（ステップＳ１００）。そして、キーボード５６０を介して暗号化コンテンツデータのライセンスを購入するための購入条件ＡＣが入力される（ステップＳ１０２）。つまり、選択した暗号化コンテンツデータを復号するライセンス鍵Ｋｃを購入するために、暗号化コンテンツデータのアクセス制限情報ＡＣｍ、および再生期限ＡＣｐを設定して購入条件ＡＣが入力される。

【０２０２】暗号化コンテンツデータの購入条件ＡＣが入力されると、コントローラ５１０は、バスＢＳ２を介してライセンス管理デバイス５２０へ認証データの出力指示を与える（ステップＳ１０４）。ライセンス管理デバイス５２０のコントローラ５２２０は、端子５２２６、インタフェース５２２４およびバスＢＳ５を介して認証データの出力指示を受取る。そして、コントローラ５２２０は、バスＢＳ５を介して認証データ保持部５２００から認証データ｛ＫＰｍ７／／Ｃｍ７｝ＫＰａ２を読出し、｛ＫＰｍ７／／Ｃｍ７｝ＫＰａ２をバスＢＳ５、インタフェース５２２４および端子５２２６を介して出力する（ステップＳ１０６）。

【０２０３】パーソナルコンピュータ５０のコントローラ５１０は、ライセンス管理デバイス５２０からの認証データ｛ＫＰｍ７／／Ｃｍ７｝ＫＰａ２に加えて、コン

テンツＩＤ、ライセンス購入条件のデータＡＣ、および配信リクエストを配信サーバ１０に対して送信する（ステップＳ１０８）。

【０２０４】配信サーバ１０では、パーソナルコンピュータ５０から配信リクエスト、コンテンツＩＤ、認証データ｛ＫＰｍ７／／Ｃｍ７｝ＫＰａ２、およびライセンス購入条件のデータＡＣを受信し（ステップＳ１１０）、復号処理部３１２においてライセンス管理デバイス５２０から出力された認証データをレベル２認証鍵ＫＰａで復号処理を実行する（ステップＳ１１２）。

【０２０５】配信制御部３１５は、復号処理部３１２における復号処理結果から、正規の機関でその正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行なう（ステップＳ１１４）。正当な認証データであると判断された場合、配信制御部３１５は、クラス公開暗号鍵ＫＰｍ７およびクラス証明書Ｃｍ７を承認し、受理する。そして、次の処理（ステップＳ１１６）へ移行する。正当な認証データでない場合には、非承認とし、クラス公開暗号鍵ＫＰｍ７およびクラス証明書Ｃｍ７を受理しないで配信セッションを終了する（ステップＳ１９８）。仮に、レベル１からの配信要求を行っていたとすると、レベル２認証鍵ＫＰａ２では、レベル１の認証データを認証することができないためここで処理は終了する。

【０２０６】認証の結果、正規の認証データであり、クラス公開暗号鍵ＫＰｍ７およびクラス証明書Ｃｍ７を承認されると、配信制御部３１５は、次に、ライセンス管理デバイスのクラス証明書Ｃｍ７が禁止クラスリストＣＲＬにリストアップされているかどうかをＣＲＬデータベース３０６に照会し、これらのクラス証明書が禁止クラスリストの対象になっている場合には、ここで配信セッションを終了する（ステップＳ１９８）。

【０２０７】一方、ライセンス管理デバイス５２０のクラス証明書が禁止クラスリストの対象外である場合には次の処理に移行する（ステップＳ１１６）。

【０２０８】認証の結果、正当な認証データを持つライセンス管理デバイスを備えるパーソナルコンピュータからのアクセスであり、クラスが禁止クラスリストの対象外であることが確認されると、配信サーバ１０において、配信制御部３１５は、配信を特定するための管理コードであるトランザクションＩＤを生成する（ステップＳ１１８）。また、セッションキー発生部３１６は、配信のためのセッションキーＫｓ１を生成する（ステップＳ１２０）。セッションキーＫｓ１は、復号処理部３１２によって得られたライセンス管理デバイス５２０に対応するクラス公開暗号鍵ＫＰｍ７によって、暗号化処理部３１８によって暗号化される（ステップＳ１２２）。

【０２０９】トランザクションＩＤおよび暗号化されたセッションキーＫｓ１は、トランザクションＩＤ／／｛Ｋｓ１｝Ｋｍ７として、バスＢＳ１および通信装置３５０を介して外部に出力される（ステップＳ１２４）。

【０２１０】図１４を参照して、パーソナルコンピュータ５０が、トランザクションＩＤ／／｛Ｋｓ１｝Ｋｍ７を受信すると（ステップＳ１２６）、コントローラ５１０は、トランザクションＩＤ／／｛Ｋｓ１｝Ｋｍ７をライセンス管理デバイス５２０に入力する（ステップＳ１２８）。そうすると、ライセンス管理デバイス５２０においては、端子５２２６およびインタフェース５２２４を介して、バスＢＳ５に与えられた受信データを、復号処理部５２２２が、保持部５２２１に保持されるライセンス管理デバイス５２０にクラス秘密復号鍵Ｋｍ７により復号処理することにより、セッションキーＫｓ１を復号し、セッションキーＫｓ１を受理する（ステップＳ１３０）。

【０２１１】コントローラ５２２０は、配信サーバ１０で生成されたセッションキーＫｓ１の受理を確認すると、セッションキー発生部５２１８に対してライセンス管理デバイス５２０において配信動作時に生成されるセッションキーＫｓ２の生成を指示する。そして、セッションキー発生部５２１８は、セッションキーＫｓ２を生成する（ステップＳ１３２）。

【０２１２】また、配信セッションにおいては、コントローラ５２２０は、ライセンス管理デバイス５２０内のメモリ５２１５に記録されている禁止クラスリストＣＲＬから更新日時ＣＲＬｄａｔｅをメモリ１４１５から抽出して切換スイッチ５２４６に出力する（ステップＳ１３４）。

【０２１３】暗号化処理部５２０６は、切換スイッチ５２４２の接点Ｐａを介して復号処理部５２２２より与えられるセッションキーＫｓ１によって、切換スイッチ５２４６の接点を順次切換えることによって与えられるセッションキーＫｓ２、個別公開暗号鍵ＫＰｍｃ８および禁止クラスリストの更新日時ＣＲＬｄａｔｅを１つのデータ列として暗号化して、｛Ｋｓ２／／ＫＰｍｃ８／／ＣＲＬｄａｔｅ｝Ｋｓ１をバスＢＳ３に出力する（ステップＳ１３６）。

【０２１４】バスＢＳ３に出力された暗号化データ｛Ｋｓ２／／ＫＰｍｃ８／／ＣＲＬｄａｔｅ｝Ｋｓ１は、バスＢＳ３からインタフェース５２２４および端子５２２６を介してパーソナルコンピュータ５０に出力され、パーソナルコンピュータ５０から配信サーバ１０に送信される（ステップＳ１３８）。

【０２１５】配信サーバ１０は、トランザクションＩＤ／／｛Ｋｓ２／／ＫＰｍｃ８／／ＣＲＬｄａｔｅ｝Ｋｓ１を受信して、復号処理部３２０においてセッションキーＫｓ１による復号処理を実行し、ライセンス管理デバイス５２０で生成されたセッションキーＫｓ２、ライセンス管理デバイス５２０固有の個別公開暗号鍵ＫＰｍｃ８およびライセンス管理デバイス５２０における禁止クラスリストの更新日時ＣＲＬｄａｔｅを受理する（ステ

ップS142）。

【0216】配信制御部315は、ステップS110で取得したコンテンツIDおよびライセンス購入条件ACに従って、アクセス制限情報ACmおよび再生期限ACpを生成する（ステップS144）。さらに、暗号化コンテンツデータを復号するためのライセンス鍵Kcを情報データベース304より取得する（ステップS146）。

【0217】配信制御部315は、生成したライセンス、すなわち、トランザクションID、コンテンツID、ライセンス鍵Kc、再生期限ACp、およびアクセス制限情報ACmを暗号化処理部326に与える。暗号化処理部326は、復号処理部320によって得られたライセンス管理デバイス520固有の個別公開暗号鍵KPmc8によってライセンスを暗号化して暗号化データ{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8を生成する（ステップS148）。

【0218】図15を参照して、配信サーバ10において、ライセンス管理デバイス520から送信された禁止クラスリストの更新日時CRLdateを、CRLデータベース306に保持される配信サーバ10の禁止クラスリストCRLの更新日時と比較することによって、ライセンス管理デバイス520は保持する禁止クラスリストCRLが最新か否かが判断され、最新と判断されたとき、ステップS152へ移行する。また、最新でないときはステップS160へ移行する（ステップS150）。

【0219】最新と判断されたとき、暗号化処理部328は、暗号化処理部326から出力された暗号化データ{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8をライセンス管理デバイス520において発生されたセッションキーKs2によって暗号化を行い、暗号化データ{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8}Ks2をバスBS1に出力する。そして、配信制御部315は、バスBS1上の暗号化データ{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8}Ks2を通信装置350を介してパーソナルコンピュータ50へ送信する（ステップS152）。

【0220】そして、パーソナルコンピュータ50のコントローラ510は、暗号化データ{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8}Ks2を受信し（ステップS154）、バスBS5を介してライセンス管理デバイス520に入力する。ライセンス管理デバイス520の復号処理部5212は、暗号化データ{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8}Ks2を端子5226およびインタフェース5224を介して受取り、セッションキー発生部5218によって発生されたセッションキーKs2によって復号し、{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8を受理する（ステップS158）。その後、ステップS172へ移行する。

【0221】一方、最新でないと判断されると、配信制御部315は、バスBS1を介してCRLデータベース306から最新の禁止クラスリストCRLを取得し、差分データである差分CRLを生成する（ステップS160）。

【0222】暗号化処理部328は、暗号化処理部326の出力と、配信制御部315がバスBS1を介して供給する禁止クラスリストの差分CRLとを受けて、ライセンス管理デバイス520において生成されたセッションキーKs2によって暗号化する。暗号化処理部328より出力された暗号化データ{差分CRL//{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8}Ks2は、バスBS1および通信装置350を介してパーソナルコンピュータ50に送信される（ステップS162）。

【0223】パーソナルコンピュータ50は、送信された暗号化データ{差分CRL//{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8}Ks2を受信し（ステップS164）、バスBS5を介してライセンス管理デバイス520に入力する（ステップS166）。ライセンス管理デバイス520においては、端子5226およびインタフェース5224を介して、バスBS5に与えられた受信データを復号処理部5212によって復号する。復号処理部5212は、セッションキー発生部5218から与えられたセッションキーKs2を用いてバスBS5の受信データを復号しバスBS5に出力する（ステップS168）。

【0224】この段階で、バスBS5には、Kmc保持部5221に保持される秘密復号鍵Kmc8で復号可能な暗号化ライセンス{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8}と、差分CRLとが出力される（ステップS168）。コントローラ5220の指示によって受理した差分CRLによってメモリ5215内のCRL領域5215Aを差分CRLに基づいて更新する（ステップS170）。

【0225】ステップS152，S154，S156，S158は、ライセンス管理デバイス520が保持する禁止クラスリストCRLが最新の場合のライセンス鍵Kc等のライセンス管理デバイス520への配信動作であり、ステップS160，S162，S164，S166，S168，S170は、ライセンス管理デバイス520が保持する禁止クラスリストCRLが最新でない場合のライセンス鍵Kc等のライセンス管理デバイス520への配信動作である。このように、ライセンス管理デバイス520から送られてきた禁止クラスリストの更新

日時ＣＲＬｄａｔｅが最新の更新日時か否かを、逐一、確認し、最新でないとき、最新の禁止クラスリストＣＲＬｄａｔｅをＣＲＬデータベース３０６から取得し、差分ＣＲＬをライセンス管理デバイス５２０に配信することによって、ライセンスの破られたライセンス管理デバイスへの配信したライセンスの流出を防止できる。

【０２２６】ステップＳ１５８またはステップＳ１７０の後、コントローラ５２２０の指示によって、暗号化ライセンス｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ８は、復号処理部５２０４において、個別秘密復号鍵Ｋｍｃ８によって復号され、ライセンス（ライセンス鍵Ｋｃ、トランザクションＩＤ、コンテンツＩＤ、アクセス制限情報ＡＣｍおよび再生期限ＡＣｐ）が受理される（ステップＳ１７２）。

【０２２７】図１６を参照して、コントローラ５１０は、ライセンス管理デバイス５２０が受理したライセンスを格納するエントリを指示するためのエントリ番号を、ライセンス管理デバイス５２０に入力する（ステップＳ１７４）。そうすると、ライセンス管理デバイス５２０のコントローラ５２２０は、端子５２２６およびインタフェース５２２４を介してエントリ番号を受取り、その受取ったエントリ番号によって指定されるメモリ５２１５のライセンス領域５２１５Ｂに、ステップＳ１７２において取得したライセンス（ライセンス鍵Ｋｃ、トランザクションＩＤ、コンテンツＩＤ、アクセス制限情報ＡＣｍおよび再生期限ＡＣｐ）を格納する（ステップＳ１７６）。

【０２２８】パーソナルコンピュータ５０のコントローラ５１０は、配信サーバ１０から送られたトランザクションＩＤと、暗号化コンテンツデータの配信要求を配信サーバ１０へ送信する（ステップＳ１７８）。

【０２２９】配信サーバ１０は、トランザクションＩＤおよび暗号化コンテンツデータの配信要求を受信し（ステップＳ１８０）、情報データベース３０４より、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆを取得して、これらのデータをバスＢＳ１および通信装置３５０を介して出力する（ステップＳ１８２）。

【０２３０】パーソナルコンピュータ５０は、｛Ｄｃ｝Ｋｃ／／Ｄｃ－ｉｎｆを受信して、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆを受理する（ステップＳ１８４）。そうすると、コントローラ５１０は、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆを１つのコンテンツファイルとしてバスＢＳ２を介してハードディスク（ＨＤＤ）５３０に記録する（ステップＳ１８６）。また、コントローラ５１０は、ライセンス管理デバイス５２０に格納されたライセンスのエントリ番号と、平文のトランザクションＩＤおよびコンテンツＩＤを含む暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆに対するライセンス管理ファイルを生成し、バスＢＳ２を介してＨＤＤ５３０に記録する（ステップＳ１８８）。さらに、コントローラ５１０は、ＨＤＤ５３０に記録されているコンテンツリストファイルに受理したコンテンツの情報として、記録したコンテンツファイル及びライセンス管理ファイルの名称や、付加情報Ｄｃ－ｉｎｆから抽出した暗号化コンテンツデータに関する情報（曲名、アーティスト名）等を追記し（ステップＳ１９０）、トランザクションＩＤと配信受理を配信サーバ１０へ送信する（ステップＳ１９２）。

【０２３１】配信サーバ１０は、トランザクションＩＤ／／配信受理を受信すると（ステップＳ１９４）、課金データベース３０２への課金データの格納、およびトランザクションＩＤの配信記録データベース３０８への記録が行われて配信終了の処理が実行され（ステップＳ１９６）、全体の処理が終了する（ステップＳ１９８）。

【０２３２】このようにして、パーソナルコンピュータ５０に内蔵されたライセンス管理デバイス５０が正規の認証データを保持する機器であること、同時に、クラス証明書Ｃｍ７とともに暗号化して送信できた公開暗号鍵ＫＰｍ７が有効であることを確認した上で、クラス証明書Ｃｍ７が禁止クラスリスト、すなわち、公開暗号鍵ＫＰｍ７による暗号化が破られたクラス証明書リストに記載されていないライセンス管理デバイスからの配信要求に対してのみコンテンツデータを配信することができ、不正なライセンス管理デバイスへの配信および解読されたクラス鍵を用いた配信を禁止することができる。

【０２３３】また、配信サーバおよびライセンス管理デバイスでそれぞれ生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、データ配信システムのセキュリティを向上させることができる。

【０２３４】また、ライセンス管理デバイス５２０は、配信サーバ１０から暗号化コンテンツデータおよびライセンスを受信する際に、配信サーバ１０との間でハード的にデータのやり取りを行ない、暗号化コンテンツデータを再生するためのライセンスをハード的に格納するため、そのセキュリティレベルは高い。したがって、ライセンス管理デバイス５２０を用いれば、パーソナルコンピュータ５０は、セキュリティレベルの高い配信によって暗号化コンテンツデータおよびライセンスを受信できるとともに、セキュリティレベルの高いレベル２ライセンスの管理が可能である。

【０２３５】［配信２］図１に示すデータ配信システムにおいて、配信サーバ１０からパーソナルコンピュータ５０のライセンス管理モジュール５１１へ暗号化コンテンツデータおよびライセンスを配信する動作について説

明する。なお、この動作を「配信２」という。

【０２３６】図１７～図２１は、図１に示すデータ配信システムにおける暗号化コンテンツデータの購入時に発生するパーソナルコンピュータ５０に内蔵されたライセンス管理モジュール５１１への配信動作を説明するための第１～第５のフローチャートである。なお、ライセンス管理モジュール５１１は、暗号化コンテンツデータおよびライセンスの配信サーバ１０からの受信をプログラムによって実行する。

【０２３７】図１７における処理以前に、パーソナルコンピュータ５０のユーザは、配信サーバ１０に対してモデム４０を介して接続し、購入を希望するコンテンツに対するコンテンツＩＤを取得していることを前提としている。

【０２３８】図１７を参照して、パーソナルコンピュータ５０のユーザからキーボード５６０を介してコンテンツＩＤの指定による配信リクエストがなされる（ステップＳ２００）。そして、キーボード５６０を介して暗号化コンテンツデータのライセンスを購入するための購入条件ＡＣが入力される（ステップＳ２０２）。つまり、選択した暗号化コンテンツデータを復号するライセンス鍵Ｋｃを購入するために、暗号化コンテンツデータのアクセス制限情報ＡＣｍ、および再生期限ＡＣｐを設定して購入条件ＡＣが入力される。

【０２３９】暗号化コンテンツデータの購入条件ＡＣが入力されると、コントローラ５１０は、ライセンス管理モジュール５１１から認証データ｛ＫＰｍ５／／Ｃｍ５｝ＫＰａ２を読出し、その読出した認証データ｛ＫＰｍ５／／Ｃｍ５｝ＫＰａ２に加えて、コンテンツＩＤ、ライセンス購入条件のデータＡＣ、および配信リクエストを配信サーバ１０に対して送信する（ステップＳ２０４）。

【０２４０】配信サーバ１０では、パーソナルコンピュータ５０から配信リクエスト、コンテンツＩＤ、認証データ｛ＫＰｍ５／／Ｃｍ５｝ＫＰａ２、およびライセンス購入条件のデータＡＣを受信し（ステップＳ２０６）、復号処理部３１２においてライセンス管理モジュール５１１から出力された認証データをレベル１認証鍵ＫＰａ１で復号処理を実行する（ステップＳ２０８）。

【０２４１】配信制御部３１５は、復号処理部３１２における復号処理結果から、処理が正常に行なわれたか否か、すなわち、正規の機関でクラス公開暗号鍵ＫＰｍ５とクラス証明書Ｃｍ５の正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行なう（ステップＳ２１０）。正当な認証データであると判断された場合、配信制御部３１５は、クラス公開暗号鍵ＫＰｍ５およびクラス証明書Ｃｍ５を承認し、受理する。そして、次の処理（ステップＳ２１２）へ移行する。正当な認証データでない場合には、非承認とし、クラス公開暗号鍵ＫＰｍ５およびクラス証明書Ｃｍ５を受理しないで処理を終了する（ステップＳ２８８）。

【０２４２】認証の結果、正規のモジュールであることが認識されると、配信制御部３１５は、次に、ライセンス管理モジュール５１１のクラス証明書Ｃｍ５が禁止クラスリストＣＲＬにリストアップされているかどうかをＣＲＬデータベース３０６に照会し、これらのクラス証明書が禁止クラスリストの対象になっている場合には、ここで配信セッションを終了する（ステップＳ２８８）。

【０２４３】一方、ライセンス管理モジュール５１１のクラス証明書が禁止クラスリストの対象外である場合には次の処理に移行する（ステップＳ２１４）。

【０２４４】認証の結果、正当な認証データを持つライセンス管理モジュールを備えるパーソナルコンピュータからのアクセスであり、クラスが禁止クラスリストの対象外であることが確認されると、配信サーバ１０において、配信制御部３１５は、配信を特定するための管理コードであるトランザクションＩＤを生成する（ステップＳ２１４）。また、セッションキー発生部３１６は、配信のためのセッションキーＫｓ１を生成する（ステップＳ２１６）。セッションキーＫｓ１は、復号処理部３１２によって得られたライセンス管理モジュール５１１に対応するクラス公開暗号鍵ＫＰｍ５によって、暗号化処理部３１８によって暗号化される（ステップＳ２１８）。

【０２４５】トランザクションＩＤおよび暗号化されたセッションキーＫｓ１は、トランザクションＩＤ／／｛Ｋｓ１｝Ｋｍ５として、バスＢＳ１および通信装置３５０を介して外部に出力される（ステップＳ２２０）。

【０２４６】図１８を参照して、パーソナルコンピュータ５０のコントローラ５１０が、トランザクションＩＤ／／｛Ｋｓ１｝Ｋｍ５を受信すると（ステップＳ２２２）、ライセンス管理モジュール５１１は、｛Ｋｓ１｝Ｋｍ５を受けて、ライセンス管理モジュール５１１に固有のクラス秘密復号鍵Ｋｍ５により復号処理して、セッションキーＫｓ１を受理する（ステップＳ２２４）。

【０２４７】ライセンス管理モジュール５１１は、配信サーバ１０で生成されたセッションキーＫｓ１の受理を確認すると、セッションキーＫｓ２を生成する（ステップＳ２２６）。そして、コントローラ５１０は、バスＢＳ２を介してＨＤＤ５３０に記憶された暗号化ＣＲＬを読出し、ライセンス管理モジュール５１１は、暗号化ＣＲＬを復号して禁止クラスリストＣＲＬを取得し、復号した禁止クラスリストＣＲＬに基づいて禁止クラスリストの更新日時ＣＲＬｄａｔｅを取得する（ステップＳ２２８）。ライセンス管理モジュール５１１は、さらに、配信サーバ１０において発生されたセッションキーＫｓ１によって、ライセンス管理モジュール５１１で発生させたセッションキーＫｓ２、個別公開暗号鍵ＫＰｍｃ６および禁止クラスリストのデータＣＲＬｄａｔｅを１つ

のデータ列として暗号化して、｛Ｋｓ２／／ＫＰｍｃ６／／ＣＲＬｄａｔｅ｝Ｋｓ１を出力する（ステップＳ２３０）。

【０２４８】コントローラ５１０は、暗号化データ｛Ｋｓ２／／ＫＰｍｃ６／／ＣＲＬｄａｔｅ｝Ｋｓ１にトランザクションＩＤを加えたトランザクションＩＤ／／｛Ｋｓ２／／ＫＰｍｃ６／／ＣＲＬｄａｔｅ｝Ｋｓ１を配信サーバ１０へ送信する（ステップＳ２３２）。

【０２４９】配信サーバ１０は、トランザクションＩＤ／／｛Ｋｓ２／／ＫＰｍｃ６／／ＣＲＬｄａｔｅ｝Ｋｓ１を受信して（ステップＳ２３４）、復号処理部３２０においてセッションキーＫｓ１による復号処理を実行し、ライセンス管理モジュール５１１で生成されたセッションキーＫｓ２、ライセンス管理モジュール５１１に固有の個別公開暗号鍵ＫＰｍｃ６およびライセンス管理モジュール５１１における禁止クラスリストの更新日時ＣＲＬｄａｔｅを受理する（ステップＳ２３６）。

【０２５０】配信制御部３１５は、ステップＳ２０６で取得したコンテンツＩＤおよびライセンス購入条件のデータＡＣに従って、アクセス制限情報ＡＣｍおよび再生期限ＡＣｐを生成する（ステップＳ２３８）。さらに、暗号化コンテンツデータを復号するためのライセンス鍵Ｋｃを情報データベース３０４より取得する（ステップＳ２４０）。

【０２５１】配信制御部３１５は、生成したライセンス、すなわち、トランザクションＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、再生期限ＡＣｐ、およびアクセス制限情報ＡＣｍを暗号化処理部３２６に与える。暗号化処理部３２６は、復号処理部３２０によって得られたライセンス管理モジュール５１１に固有の個別公開暗号鍵ＫＰｍｃ６によってライセンスを暗号化して暗号化データ｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ６を生成する（ステップＳ２４２）。

【０２５２】図１９を参照して、配信サーバ１０において、ライセンス管理モジュール５１１から送信された禁止クラスリストの更新日時ＣＲＬｄａｔｅによって、配信を求めてきたライセンス管理デバイス５２０の禁止クラスリストＣＲＬが最新か否かが判断され、ライセンス管理モジュールの禁止クラスリストＣＲＬが最新と判断されたとき、ステップＳ２４６へ移行する。また、最新でないと判断されたときはステップＳ２５２へ移行する（ステップＳ２４４）。

【０２５３】最新と判断されたとき、暗号化処理部３２８は、暗号化処理部３２６から出力された暗号化データ｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ６をライセンス管理モジュール５１１において発生されたセッションキーＫｓ２によって暗号化を行い、暗号化データ｛｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ６｝Ｋｓ２をバスＢＳ１に出力する。そして、配信制御部３１５は、バスＢＳ１上の暗号化データ｛｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ６｝Ｋｓ２を通信装置３５０を介してパーソナルコンピュータ５０へ送信する（ステップＳ２４６）。

【０２５４】そして、パーソナルコンピュータ５０のコントローラ５１０は、暗号化データ｛｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ６｝Ｋｓ２を受信し（ステップＳ２４８）、ライセンス管理モジュール５１１は、暗号化データ｛｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ６｝Ｋｓ２をセッションキーＫｓ２によって復号し、｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ６を受理する（ステップＳ２５０）。その後、ステップＳ２６２へ移行する。

【０２５５】一方、最新でないと判断されると、配信制御部３１５は、バスＢＳ１を介してＣＲＬデータベース３０６から最新の禁止クラスリストＣＲＬを取得し、差分データである差分ＣＲＬを生成する（ステップＳ２５２）。

【０２５６】暗号化処理部３２８は、暗号化処理部３２６の出力と、配信制御部３１５がバスＢＳ１を介して供給する禁止クラスリストの差分ＣＲＬとを受けて、ライセンス管理モジュール５１１において生成されたセッションキーＫｓ２によって暗号化する。暗号化処理部３２８より出力された暗号化データ｛差分ＣＲＬ／／｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ６｝Ｋｓ２は、バスＢＳ１および通信装置３５０を介してパーソナルコンピュータ５０に送信される（ステップＳ２５４）。

【０２５７】パーソナルコンピュータ５０は、送信された暗号化データ｛差分ＣＲＬ／／｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ６｝Ｋｓ２を受信し（ステップＳ２５６）、ライセンス管理モジュール５１１は、セッションキーＫｓ２を用いて受信データを復号して差分ＣＲＬと暗号化データ｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ６と受理する（ステップＳ２５８）。

【０２５８】コントローラ５１０は、ＨＤＤ５３０に記録された禁止クラスリストＣＲＬに受理した差分ＣＲＬを加え、独自の暗号処理を施し、ＨＤＤ５３０内の禁止クラスリストＣＲＬを書換える（ステップＳ２６０）。

【０２５９】ステップＳ２４６，Ｓ２４８，Ｓ２５０は、ライセンス管理モジュール５１１から送られてきた禁止クラスリストの更新日時ＣＲＬｄａｔｅによって、ライセンス管理モジュール５１１の管理する禁止クラスリストＣＲＬが最新の場合のライセンスのライセンス管

理モジュール５１１への配信動作であり、ステップＳ２５２，Ｓ２５４，Ｓ２５６，Ｓ２５８，Ｓ２６０は、禁止クラスリストＣＲＬが最新でない場合のライセンスのライセンス管理モジュール５１１への配信動作である。このように、ライセンス管理モジュール５１１から送られてきた禁止クラスリストの更新日時ＣＲＬｄａｔｅによって、配信を求めてきたライセンス管理デバイス５２０の禁止クラスリストＣＲＬが最新か否かを、逐一、確認し、最新でないとき、最新の禁止クラスリストＣＲＬをＣＲＬデータベース３０６から取得し、差分ＣＲＬをライセンス管理モジュール５１１に配信することによって、ライセンス管理モジュールへ配信したライセンスがセキュリティの破られた機器へ流出されるのを防止できる。

【０２６０】ステップＳ２５０またはステップＳ２６０の後、暗号化ライセンス｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ６は、個別秘密復号鍵Ｋｍｃ６によって復号され、ライセンス（ライセンス鍵Ｋｃ、トランザクションＩＤ、コンテンツＩＤ、アクセス制限情報ＡＣｍおよび再生期限ＡＣｐ）が受理される（ステップＳ２６２）。

【０２６１】このように、配信サーバおよびライセンス管理モジュールでそれぞれ生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、データ配信システムのセキュリティを向上させることができる。

【０２６２】ライセンス管理モジュール５１１は、受理したアクセス制限情報ＡＣｍによって再生回数が制限されているか否かを判別し、再生回数が制限されていないときステップＳ２６６へ移行し、再生回数が制限されているときステップＳ２６８へ移行する（ステップＳ２６４）。そして、再生回数が制限されていなとき、ライセンス管理モジュール５１１は、配信サーバ１０から受信した暗号化コンテンツおよびライセンスを他の装置へ貸出すためのチェックアウト可能数を含むチェックアウト情報を生成する（ステップＳ２６６）。この場合、チェックアウトの初期値は「３」に設定される。また、再生回数が制限されているとき、ライセンス管理モジュール５１１は、暗号化コンテンツデータを他の装置へ貸出すためのチェックアウト可能数を「０」に設定してチェックアウト情報を生成する（ステップＳ２６８）。ステップＳ２６８は、チェックアウトすることで再生回数の管理ができないための処理である。

【０２６３】図２０を参照して、ステップＳ２６６またはステップＳ２６８の後、ライセンス管理モジュール５１１は、認証データ｛ＫＰｍ５／／Ｃｍ５｝ＫＰａ１をバス２を介してライセンス管理デバイス５２０へ出力する（ステップＳ２７０）。ライセンス管理デバイス５２０では、ライセンス管理モジュール５１１から認証データ｛ＫＰｍ５／／Ｃｍ５｝ＫＰａ１を受信し、復号処理部５２０８は、認証データ認証データ｛ＫＰｍ５／／Ｃｍ５｝ＫＰａ１を受取って、認証データ認証データ｛ＫＰｍ５／／Ｃｍ５｝ＫＰａ１に基づいて、ＫＰａ保持部５２１４からレベル１認証鍵ＫＰａ１を受取り、受取ったレベル１認証鍵ＫＰａ１によって認証データ｛ＫＰｍ５／／Ｃｍ５｝ＫＰａ１を復号する（ステップＳ２７１）。

【０２６４】コントローラ５２２０は、復号処理部５２０８における復号処理結果から、処理が正常に行なわれたか否か、すなわち、正規の機関でクラス公開暗号鍵ＫＰｍ５とクラス証明書Ｃｍ５との正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行なう（ステップＳ２７２）。正当な認証データであると判断された場合、コントローラ５２２０は、クラス公開暗号鍵ＫＰｍ５およびクラス証明書Ｃｍ５を承認し、受理する。そして、次の処理（ステップＳ２７３）へ移行する。正当な認証データでない場合には、非承認とし、クラス公開暗号鍵ＫＰｍ５およびクラス証明書Ｃｍ５を受理しないで処理を終了する（ステップＳ２９８）。

【０２６５】認証の結果、正規の認証データを受信したことが認識されると、コントローラ５２２０は、次に、ライセンス管理モジュール５１１のクラス証明書Ｃｍ５が禁止クラスリストＣＲＬにリストアップされているかどうかをメモリ５２１５のＣＲＬ領域５２１５Ａに照会し、これらのクラス証明書が禁止クラスリストの対象になっている場合には、ここで配信セッションを終了する（ステップＳ２９８）。

【０２６６】一方、ライセンス管理モジュール５１１のクラス証明書が禁止クラスリストの対象外である場合には次の処理に移行する（ステップＳ２７３）。

【０２６７】認証の結果、正当な認証データを持つライセンス管理デバイスを備えるライセンス管理モジュール５１１からのアクセスであり、クラスが禁止クラスリストの対象外であることが確認されると、ライセンス管理デバイス５２０において、セッションキー発生部５２０８は、セッションキーＫｓ２ａを生成し（ステップＳ２７４）、暗号処理部５２１０は、セッションキーＫｓ２ａをクラス公開暗号鍵ＫＰｍ５によって暗号化して暗号化データ｛Ｋｓ２ａ｝Ｋｍ５を出力する（ステップＳ２７５）。

【０２６８】コントローラ５２２０は、暗号化データ｛Ｋｓ２ａ｝Ｋｍ５をバスＢＳ５、インタフェース５２２４、および端子５２２６を介して出力し、ライセンス管理モジュール５１１は、バスＢＳ２を介して暗号化データ｛Ｋｓ２ａ｝Ｋｍ５を受信し、クラス秘密復号鍵Ｋｍ５によって暗号化データ｛Ｋｓ２ａ｝Ｋｍ５を復号してセッションキーＫｓ２ａを受理する（ステップＳ２７

６）。そして、ライセンス管理モジュール５１１は、セッションキーＫｓ２ｂを生成し（ステップＳ２７７）、セッションキーＫｓ２ｂをセッションキーＫｓ２ａによって暗号化して暗号化データ｛Ｋｓ２ｂ｝Ｋｓ２ａをバスＢＳ２を介してライセンス管理デバイス５２０へ出力する（ステップＳ２７８）。

【０２６９】ライセンス管理デバイス５２０のコントローラ５２２０は、端子５２２６、インタフェース５２２４、およびバスＢＳ５を介して暗号化データ｛Ｋｓ２ｂ｝Ｋｓ２ａを受け、復号処理部５２１２は、セッションキー発生部５２０８から出力されるセッションキーＫｓ２ａによって暗号化データ｛Ｋｓ２ｂ｝Ｋｓ２ａを復号してセッションキーＫｓ２ｂを受理する（ステップＳ２７９）。そうすると、ライセンス管理モジュール５１１は、エントリ番号「０」をライセンス管理デバイス５２０へ入力し（ステップＳ２８０）、ライセンス管理デバイス５２０のコントローラ５２２０は、端子５２２６、インタフェース５２２４、およびバスＢＳ５を介してエントリ番号「０」を受取る。そして、コントローラ５２２０は、メモリ５２１５のライセンス領域５２１５Ｂのうち、エントリ番号「０」によって指定されている領域に格納されているバインディングライセンス（トランザクションＩＤｂ、コンテンツＩＤｂ、バインディング鍵Ｋｂ、および制御情報ＡＣｍｂ，ＡＣｐｂ）を取得する（ステップＳ２８１）。そして、コントローラ５２２０は、制御情報ＡＣｍｂに基づいてバインディングライセンスが有効か否かを判別し、有効でない場合、ステップＳ２９８へ移行し、配信セッションが終了する。ここで、有効な場合とは、制御情報ＡＣｍｂ内の再生回数が０でないこと、かつ、レベル１認証鍵ＫＰａ１によって認証された処理であるため制御情報ＡＣｍｂのセキュリティレベルがレベル１であることを意味する。

【０２７０】一方、バインディングライセンスが有効な場合、ステップＳ２８３へ移行する（ステップＳ２８２）。

【０２７１】ステップＳ２８２において、バインディングライセンスが有効と判断されると、暗号処理部５２０６は、切換スイッチ５２４６を介して取得したバインディング鍵Ｋｂおよび制御情報ＡＣｐｂを、復号処理部５２１２によって復号され、スイッチ５２４２を介して取得したセッションキーＫｓ２ｂによって暗号化して暗号化データ｛Ｋｂ／／ＡＣｐｂ｝Ｋｓ２ｂを出力する（ステップＳ２８３）。

【０２７２】図２１を参照して、コントローラ５２２０は、暗号化データ｛Ｋｂ／／ＡＣｐｂ｝Ｋｓ２ｂをバスＢＳ５、インタフェース５２２４、および端子５２２６を介して出力し、ライセンス管理モジュール５１１は、バスＢＳ２を介して暗号化データ｛Ｋｂ／／ＡＣｐｂ｝Ｋｓ２ｂを受信し、セッションキーＫｓ２ｂによって暗号化データ｛Ｋｂ／／ＡＣｐｂ｝Ｋｓ２ｂを復号してバインディング鍵Ｋｂおよび制御情報ＡＣｐｂを取得する（ステップＳ２８４）。

【０２７３】ステップＳ２７０からステップＳ２８４の一連の処理はバインディング鍵Ｋｂをライセンス管理デバイス５２０から取得する処理であり、「バインディング鍵取得処理」と総称する。

【０２７４】そして、ライセンス管理モジュール５１１は、バスＢＳ２を介してＨＤＤ５３０から暗号化機密ファイル１６０を取得し、その取得した暗号化機密ファイル１６０をバインディング鍵Ｋｂによって復号して平文の機密ファイルを取得する（ステップＳ２８５）。そうすると、ライセンス管理モジュール５１１は、配信サーバ１０から受理したライセンス（トランザクションＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、アクセス制限情報ＡＣｍ、および再生期限ＡＣｐ）とステップＳ２６６またはステップＳ２６８において生成されたチャックアウト情報とを機密情報ｎとして平文の機密ファイルに追記する（ステップＳ２８６）。その後、ライセンス管理モジュール５１１は、平文の機密ファイルをバインディング鍵Ｋｂによって再び暗号化し、その暗号化した暗号化機密ファイル１６０によってＨＤＤ５３０に記録された暗号化機密ファイル１６０を更新する（ステップＳ２８７）。ライセンスを暗号化機密ファイル１６０に格納した後、ライセンス管理モジュール５１１は、配信サーバ１０から送られたトランザクションＩＤと、暗号化コンテンツデータの配信要求を配信サーバ１０へ送信する（ステップＳ２８８）。

【０２７５】配信サーバ１０は、トランザクションＩＤおよび暗号化コンテンツデータの配信要求を受信し（ステップＳ２８９）、情報データベース３０４より、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆを取得して、これらのデータをバスＢＳ１および通信装置３５０を介して出力する（ステップＳ２９０）。

【０２７６】ライセンス管理モジュール５１１は、｛Ｄｃ｝Ｋｃ／／Ｄｃ－ｉｎｆを受信して、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆを受理する（ステップＳ２９１）。そして、ライセンス管理モジュール５１１は、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆをバスＢＳ２を介してコンテンツファイルとしてハードディスク（ＨＤＤ）５３０に記録する（ステップＳ２９２）。また、ライセンス管理モジュール５１１は、暗号化機密ファイル１６０に格納した機密情報ｎの機密情報番号ｎと、平文のトランザクションＩＤおよびコンテンツＩＤとを含むコンテンツファイル（暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆ）に対応するライセンス管理ファイルを生成し、バスＢＳ２を介してＨＤＤ５３０に記録する（ステップＳ２９３）。さらに、ライセンス管理モジュール５１１は、ＨＤＤ５３０に記録されているコン

テンツリストファイルに受理したコンテンツ情報として、記録したコンテンツファイルおよびライセンス管理ファイルの名称や、付加情報Ｄｃ－ｉｎｆから抽出した暗号化コンテンツデータに関する情報（曲名、アーティスト名）等を追記し（ステップＳ２９４）、トランザクションＩＤと配信受理を配信サーバ１０へ送信する（ステップＳ２９５）。

【０２７７】配信サーバ１０は、トランザクションＩＤ／／配信受理を受信すると（ステップＳ２９６）、課金データベース３０２への課金データの格納、およびトランザクションＩＤの配信記録データベース３０８への記録が行なわれて配信終了の処理が実行され（ステップＳ２９７）、全体の処理が終了する（ステップＳ２９８）。

【０２７８】このように、ライセンス管理モジュール５１１は、配信サーバ１０との間でソフトウエアによってデータのやり取りを行ない、暗号化コンテンツデータおよびライセンスをソフト的に配信サーバ１０から受信する。また、受信した暗号化コンテンツデータをＨＤＤ５３０に記録し、ライセンスを機密情報ｎとして機密ファイルに書込み、その機密ファイルをバインディング鍵Ｋｂによって暗号化して暗号化機密ファイル１６０にライセンスを格納する。そして、暗号化機密ファイル１６０を復号するバインディング鍵Ｋｂはライセンス管理デバイス５２０に保持される。したがって、ライセンス管理モジュール５１１による暗号化コンテンツデータおよびライセンスの配信は、ライセンス管理デバイス５２０による暗号化コンテンツデータおよびライセンスの配信よりもセキュリティレベルは低いが、記録管理においてはパーソナルコンピュータ５０に関連付けていない点において、それに近いものになる。

【０２７９】［リッピング］パーソナルコンピュータ５０のユーザは配信によって暗号化コンテンツとライセンスを取得するほかに、所有する音楽ＣＤから、音楽データを取得して利用することが可能である。著作権者の権利保護の立場から音楽ＣＤのデジタル複製は自由に行って良いものではないが、個人が自己の使用目的のために、著作権保護機能を備えるツールを用いて複製し、音楽を楽しむことは許されている。そこで、ライセンス管理モジュール５１１は、音楽ＣＤから音楽データを取得して、ライセンス管理モジュール５１１にて管理可能な暗号化コンテンツデータとライセンスを生成するリッピング機能を実現するプログラムも含んでいる。

【０２８０】また、近年の音楽ＣＤには、音楽データ内に、ウォーターマークと呼ばれる電子すかしを挿入したものがある。このウォーターマークには、著作権者が利用者における利用の範囲が利用規則として書込まれている。利用規則が書込まれている音楽データからのリッピングでは、著作権保護の点から必ずこの利用規則に従う必要がある。以後、利用規則として、複製条件（複製禁止／一世代複製可／複製可」および最大チェックアウト数が記載されているとする。また、ウォーターマーク検出されない場合、すなわち、利用規則が書込まれていない従来の音楽ＣＤであっても、著作権者の権利を保護するために、一世代の複製ができ、最大チェックアウト数が「３」と解釈するものとする。

【０２８１】図２２～図２４を参照して、音楽データが記録された音楽ＣＤからのリッピングによる暗号化コンテンツデータおよびライセンスの取得について説明する。

【０２８２】図２２～図２４は、音楽ＣＤからリッピングによって暗号化コンテンツデータおよびライセンスを取得するための第１～第３のフローチャートである。

【０２８３】図２２を参照して、リッピング動作が開始されると、ＣＤ－ＲＯＭドライブ５４０が音楽ＣＤから検出した音楽データを取り込んで、取込んだ音楽データからウォーターマークによって記載された利用規則の検出が行なわれる（ステップＳ７００）。そして、検出された利用規則に基づいて複製が可能か否かが判定される（ステップＳ７０１）。利用規則の複製条件が無制限の場合、ステップＳ２０３へ、複製条件が一世代複製可の場合、ステップＳ７０２へ移行し、複製条件が複製禁止の場合、複製が禁止され、ステップＳ７３３へ移行してリッピング動作は終了する。さらに、装着されたＣＤにウォーターマークが含まれず、利用規則が得られない場合、ステップＳ７０５へ移行する。

【０２８４】ステップＳ７０１において、利用規則の複製条件が一世代複製可の場合、ライセンス管理モジュール５１１は、取得した音楽データに含まれるウォーターマークを取得した利用規則の複製条件を複製禁止に変更したウォーターマークに付け替える（ステップＳ７０２）。そして、ステップＳ７０３へ移行する。複製ができる利用規則が検出された場合にステップＳ７０３において、ライセンス管理モジュール５１１は、利用規則を反映したアクセス制限情報ＡＣｍおよび再生期限ＡＣｐを生成する（ステップＳ７０３）。ここでも、複製条件に従い、複製可であれば、アクセス制限情報ＡＣｍの移動複製フラグを移動複製可（＝３）に設定し、一世代複製可であれば、リッピング自身が一世代に当たるので移動複製禁止（＝０）に設定する。また、対応する利用規則はないが再生回数は無制限、セキュリティレベルはレベル１に設定する。その後、ライセンス管理うモジュール５１１は、利用規則の最大チェックアウト数を反映してチェックアウト可能数を設定する。最大チェックアウト数の指定がないときはチェックアウト可能数＝３とする。そして、設定したチェックアウト可能数を含むチェックアウト情報を生成する（ステップＳ７０４）。

【０２８５】一方、ステップＳ７０１において、ウォーターマークが検出されず、利用規則が無いと判定された場合、ライセンス管理モジュール５１１は、アクセス制

限情報ＡＣｍの移動複製フラグを移動複製禁止（＝０）、再生回数は無制限（＝２５５）、セキュリティレベルは１に設定する。再生期限ＡＣｐは再生を無期限とする（ステップＳ７０５）。その後、ライセンス管理モジュール５１１は、初期値が３であるチェックアウト可能数を含むチェックアウト情報を生成する（ステップＳ７０６）。

【０２８６】ステップＳ７０４またはＳ７０６の後、ライセンス管理モジュール５１１は、乱数などによってライセンス鍵Ｋｃを生成し（ステップＳ７０７）、ローカル使用のトランザクションＩＤおよびコンテンツＩＤを生成する（ステップＳ７０８）。次に、ライセンス管理モジュール５１１は、バインディング鍵取得処理を行う。図２３のステップＳ７０９から図２４のステップ７２３の一連の処理がバインディング鍵取得処理であり、配信２の配信処理における図２０のステップＳ２７０から図２１のステップＳ２８４の一連の処理と同じである。ゆえに、説明を省略する。

【０２８７】図２４を参照して、バインディング鍵Ｋｂを取得したライセンス管理モジュール５１１は、バスＢＳ２を介してＨＤＤ５３０から暗号化機密ファイル１６０を取得し、その取得した暗号化機密ファイル１６０をバインディング鍵Ｋｂによって復号して平文の機密ファイルを取得する（ステップＳ７２４）。そうすると、ライセンス管理モジュール５１１は、音楽ＣＤから取得した音楽データを所定の方式に符号化してコンテンツデータＤｃを生成し（ステップＳ７２５）、コンテンツデータをライセンス鍵Ｋｃによって暗号化して暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを生成する（ステップＳ７２６）。その後、ライセンス管理モジュール５１１は、キーボード５６０を介して入力されたユーザからの情報、および音楽ＣＤからの情報に基づいて、コンテンツデータの付加情報Ｄｃ－ｉｎｆを生成し（ステップＳ７２７）、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆとをバスＢＳ２を介してコンテンツファイルとしてＨＤＤ５３０に記録する（ステップＳ７２８）。

【０２８８】そうすると、ライセンス管理モジュール５１１は、生成したライセンス（トランザクションＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、アクセス制限情報ＡＣｍ、および再生期限ＡＣｐ）とステップＳ７０４またはステップＳ７０６において生成されたチェックアウト情報とを機密情報ｎとして平文の機密ファイルに追記する（ステップＳ７２９）。その後、ライセンス管理モジュール５１１は、平文の機密ファイルをバインディング鍵Ｋｂによって暗号化し、その暗号化した暗号化機密ファイル１６０によってＨＤＤ５３０に記録された暗号化機密ファイル１６０を更新する（ステップＳ７３０）。ライセンスを暗号化機密ファイル１６０に格納した後、ライセンス管理モジュール５１１は、暗号化機密ファイル１６０に格納した機密情報ｎの機密情報番号ｎと、平文のトランザクションＩＤおよびコンテンツＩＤとを含むコンテンツファイル（暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆ）に対するライセンス管理ファイルを生成し、バスＢＳ２を介してＨＤＤ５３０に記録する（ステップＳ７３１）。さらに、ライセンス管理モジュール５１１は、ＨＤＤ５３０に記録されているコンテンツリストファイルに受理したコンテンツの情報として、記録したコンテンツファイル及びライセンス管理ファイルの名称や、付加情報Ｄｃ－ｉｎｆから抽出した暗号化コンテンツデータに関する情報（曲名、アーティスト名）等を追記し（ステップＳ７３２）、全体の処理が終了する（ステップＳ７３３）。

【０２８９】このように音楽ＣＤからリッピングによっても暗号化コンテンツデータとライセンスとを取得できる。そして、音楽ＣＤからのリッピングによって取得された暗号化コンテンツデータおよびライセンスは、配信によって取得された暗号化コンテンツデータおよびレベル１ライセンスと同じ方式によって、ライセンス管理モジュール５１１によって管理される。

【０２９０】図２５を参照して、パーソナルコンピュータ５０のライセンス管理モジュール５１１またはライセンス管理デバイス５２０によって受信された暗号化コンテンツデータおよびライセンスの管理について説明する。パーソナルコンピュータ５０のＨＤＤ５３０は、コンテンツリストファイル１５０と、コンテンツリストファイル１５０は、コンテンツファイル１５３１～１５３ｎと、ライセンス管理ファイル１５２１～１５２ｎと、暗号化機密ファイルとを含む。

【０２９１】コンテンツリストファイル１５０は、所有するコンテンツの一覧形式のデータファイルであり、個々のコンテンツに対する情報（楽曲名、アーティスト名など）と、コンテンツファイルとライセンス管理ファイルを示す情報（ファイル名）などが含まれている。個々のコンテンツに対する情報は受信時に付加情報Ｄｃ－ｉｎｆから必要な情報を取得して自動的に、あるいは、ユーザの指示によって記載される。また、コンテンツファイルのみ、ライセンス管理ファイルのみの再生できないコンテンツについても一覧の中で管理することが可能である。

【０２９２】コンテンツファイル１５３１～１５３ｎは、ライセンス管理モジュール５１１またはライセンス管理デバイス５２０によって受信された暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆとを記録するファイルであり、コンテンツごとに設けられる。

【０２９３】また、ライセンス管理ファイル１５２１～１５２ｎは、それぞれ、コンテンツファイル１５３１～１５３ｎに対応して記録されており、ライセンス管理モジュール５１１またはライセンス管理デバイス５２０によって受信されたライセンスを管理するためのファイルであり、ライセンスの格納場所を特定するための情報と

ライセンスに関する情報を含む。

【０２９４】格納場所を特定するための情報とは、ライセンス管理デバイス５２０にライセンスが記録された場合にはエントリ番号、もしくは暗号化機密ファイル内に記録された機密情報を特定する機密情報番号を言う。

【０２９５】ライセンスに関する情報とは、ライセンスを受信したときに平文にて参照できるトランザクションＩＤ、コンテンツＩＤや、ライセンス購入条件ＡＣから容易に判断できるアクセス制限情報ＡＣｍおよび再生制御情報ＡＣｐにて制限されている事項の平文の写しである。これまで説明でも明らかなように、ライセンスは、コンテンツ保護のために参照することができないように保護され、記録されている。しかし、ライセンス鍵Ｋｃを除く他の情報は、書き換えることさえできなければ、その内容が参照されてもコンテンツ保護の立場から何ら問題はない。アプリケーションプログラムにおいて、このライセンスに関する情報を参照して各処理を開始する。

【０２９６】暗号化機密情報ファイルは、ライセンス管理モジュール５１１にて管理されているライセンスやチェックアウト情報などを含む機密情報を含む。暗号化機密情報ファイルは、バインディング鍵Ｋｂにて暗号化されている。

【０２９７】図２５を参照して、具体的に説明する。ライセンス管理ファイル１５２１，１５２４は、それぞれ、エントリ番号１，ｍを含む。これは、ライセンス管理デバイス５２０によって受信され、ライセンス管理デバイス５２０のメモリ５２１５のライセンス領域５２１５Ｂにおいて管理されるライセンス（ライセンスＩＤ、ライセンス鍵Ｋｃ、アクセス制限情報ＡＣｍおよび再生期限ＡＣｍ）の管理領域を指定する番号である。

【０２９８】したがって、コンテンツファイル１５３１に記録されたファイル名の暗号化コンテンツデータを再生端末１００に装着されたメモリカード１１０へ移動させるとき、コンテンツファイル１５３１～１５３ｎを検索してコンテンツファイル１５３１を抽出すれば、暗号化コンテンツデータを再生するライセンスがどこで管理されているかが解かる。コンテンツファイル１５３１に対応するライセンス管理ファイル１５２１に含まれるエントリ番号は「１」であるので、コンテンツファイル１５３１に記録されたファイル名の暗号化コンテンツデータを再生するライセンスは、ライセンス管理デバイス５２０のメモリ５２１５のライセンス領域５２１５Ｂのエントリ番号１によって指定された領域に記録されている。そうすると、ＨＤＤ５３０に記録されたコンテンツリストファイル１５０のライセンス管理ファイル１５２１からエントリ番号１を読出し、その読出したエントリ番号１をライセンス管理デバイス５２０に入力することによって、メモリ５２１５のライセンス領域５２１５Ｂからライセンスを容易に取出し、メモリカード１１０へ移動できる。そして、ライセンスを移動した後は、メモリ５２１５のライセンス領域５２１５Ｂにおいて指定されたエントリ番号１内のライセンスは削除されるので、それに対応してライセンス管理ファイル１５２３のように「ライセンス無」が記録される。

【０２９９】また、ライセンス管理モジュール５１１によって受信された暗号化コンテンツデータのライセンスを格納する機密情報は、ライセンス管理ファイル１５２２，１５２４，・・・，１５２ｎによって管理される。ライセンス管理ファイル１５２２，・・・，１５２ｎは、ライセンス管理モジュール５１１によって受信した暗号化コンテンツデータを再生するためのライセンスを格納する機密情報の機密情報番号を含む。

【０３００】そうすると、たとえば、コンテンツファイル１５３２に記録されたファイル名の暗号化コンテンツデータをパーソナルコンピュータ８０へ移動させるとき、コンテンツファイル１５３１～１５３ｎを検索してコンテンツファイル１５３２を抽出し、コンテンツファイル１５３２に対応するライセンス管理ファイル１５２２から機密情報番号１を取得する。一方、ライセンス管理デバイス５２０からバインディング鍵Ｋｂを取得し、その取得したバインディング鍵Ｋｂによって暗号化機密ファイル１６０を復号して平文の機密ファイルを取得する。そうすると、ライセンス管理ファイルから取得した機密情報番号１に対応する機密ファイル中の機密情報１に格納されているライセンスを取得することができる。

【０３０１】このように、本発明の実施の形態１においては、ライセンス管理モジュール５１１によって受信した暗号化コンテンツデータのライセンスは、暗号化機密ファイル１６０に機密情報ｎとして格納されており、暗号化機密ファイル１６０は、ライセンス管理デバイス５２０によってハード的に保持されたバインディング鍵Ｋｂによってのみ復号可能である。つまり、バインディング鍵Ｋｂは、暗号化コンテンツデータのライセンスを管理する共通鍵であり、バインディング鍵Ｋｂがないとライセンスを取得することができない構造になっている。したがって、ライセンス管理モジュール５１１によって受信された暗号化コンテンツデータのライセンスは、暗号化機密ファイル１６０に書込まれてＨＤＤ５３０に記録されているため、実際はソフト的に管理されているが、ライセンス管理デバイス５２０に格納されたバインディング鍵Ｋｂがないとライセンスを暗号化機密ファイル１６０から取出すことができないわけでわるから、実質的には、ハードウエアによって管理されているのに近い。

【０３０２】一方、ライセンス管理デバイス５２０によって受信されたライセンスは、メモリ５２１５のライセンス領域５２１５Ｂに格納されている。したがって、本発明の実施の形態１によって、ライセンス管理モジュール５１１によって受信されたライセンスの管理レベル

を、ライセンス管理デバイス５２０によって受信されたライセンスの管理レベルに近づけることができる。

【０３０３】なお、バインディングライセンスは、エントリ番号「０」に格納されている物としている。

【０３０４】［移動１］図１に示すデータ配信システムにおいて、配信サーバ１０からパーソナルコンピュータ５０のライセンス管理デバイス５２０へ配信された暗号化コンテンツデータおよびライセンスを再生端末１００に装着されたメモリカード１１０へ送信する動作について説明する。なお、この動作を「移動１」という。移動は、セキュリティレベルがレベル２間でのみ行われる処理である図２６～図２９は、図１に示すデータ配信システムにおいて、ライセンス管理デバイス５２０が配信サーバ１０から受信した暗号化コンテンツデータおよびライセンスを再生端末１００に装着されたメモリカード１１０へ移動する移動動作を説明するための第１～第４のフローチャートである。

【０３０５】なお、図１８における処理以前に、パーソナルコンピュータ５０のユーザは、コンテンツリストファイルに従って、移動するコンテンツを決定し、ＨＤＤ５３０のコンテンツファイルおよびライセンス管理ファイルが特定でき、メモリカード１１０の再生リストファイルを取得していることを前提として説明する。

【０３０６】図２６を参照して、パーソナルコンピュータ５０のキーボード５６０から移動リクエストが入力されると（ステップＳ３００）、コントローラ５１０は、認証データの送信要求ａをＵＳＢインタフェース５５０、端子５８０、およびＵＳＢケーブル７０を介して再生端末１００へ送信する（ステップＳ３０２）。そうすると、再生端末１００のコントローラ１１０６は、端子１１１４、ＵＳＢインタフェース１１１２およびバスＢＳ３を介して認証データの送信要求を受信し、バスＢＳ３およびメモリカードインタフェース１２００を介して認証データの送信要求をメモリカード１１０へ送信する。そして、メモリカード１１０のコントローラ１４２０は、端子１４２６、インタフェース１４２４およびバスＢＳ４を介して認証データの送信要求を受信する（ステップＳ３０４）。

【０３０７】コントローラ１４２０は、認証データの送信要求を受信すると、認証データ保持部１４００から認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａ２をバスＢＳ４を介して読出し、その読出した認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａ２をバスＢＳ４、インタフェース１４２４および端子１４２６を介して再生端末１００へ出力する。そして、再生端末１００のコントローラ１１０６は、メモリカードインタフェース１２００およびバスＢＳ３を介して認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａ２を受取り、バスＢＳ３、ＵＳＢインタフェース１１１２、端子１１１４およびＵＳＢケーブル７０を介してパーソナルコンピュータ５０へ認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａ２を送信する（ステップＳ３０６）。

【０３０８】そうすると、パーソナルコンピュータ５０のコントローラ５１０は、端子５８０およびＵＳＢインタフェース５５０を介して認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａ２を受信し（ステップＳ３０８）、その受信した認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａ２をバスＢＳ２を介してライセンス管理デバイス５２０へ送信する。ライセンス管理デバイス５２０のコントローラ５２２０は、端子５２２６、インタフェース５２２４、およびバスＢＳ５を介して認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａ２を受信し、その受信した認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａ２を復号処理部５２０８へ与える。認証処理部５２０８は、ＫＰａ保持部５２１４は、認証データ認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａ２を受取って、認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａ２に基づいて、ＫＰａ保持部５２１４からレベル２認証鍵ＫＰａ２を受取り、その受取ったレベル２認証鍵ＫＰａ２によって認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａ２の復号処理を実行する（ステップＳ３１０）。コントローラ５２２０は、復号処理部５２０８における復号処理結果から、処理が正常に行なわれたか否か、すなわち、メモリカード１１０が正規のメモリカードからのクラス公開暗号鍵ＫＰｍ３とクラス証明書Ｃｍ３とを保持することを認証するために、正規の機関でその正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行なう（ステップＳ３１２）。正当な認証データであると判断された場合、コントローラ５２２０は、クラス公開暗号鍵ＫＰｍ３およびクラス証明書Ｃｍ３を承認し、受理する。そして、次の処理（ステップＳ３１４）へ移行する。正当な認証データでない場合には、非承認とし、クラス公開暗号鍵ＫＰｍ３およびクラス証明書Ｃｍ３を受理しないで処理を終了する（ステップＳ４０４）。

【０３０９】認証の結果、正規のメモリカードであることが認識されると、コントローラ５２２０は、次に、メモリカード１１０のクラス証明書Ｃｍ３が禁止クラスリストＣＲＬにリストアップされているかどうかをメモリ５２１５のＣＲＬ領域５２１５Ａに照会し、これらのクラス証明書が禁止クラスリストの対象になっている場合には、ここで移動動作を終了する（ステップＳ４０４）。

【０３１０】一方、メモリカード１１０のクラス証明書が禁止クラスリストの対象外である場合には次の処理に移行する（ステップＳ３１４）。

【０３１１】認証の結果、正当な認証データを持つメモリカードを備える再生端末からのアクセスであり、クラスが禁止クラスリストの対象外であることが確認されると、ライセンス管理デバイス５２０において、コントローラ５２２０は、移動を特定するための管理コードであるトランザクションＩＤをメモリ５２１５のライセンス

領域５２１５Ｂから取得する（ステップＳ３１６）。そして、セッションキー発生部５２１８は、移動のためのセッションキーＫｓ２２を生成する（ステップＳ３１８）。セッションキーＫｓ２２は、復号処理部５２０８によって得られたメモリカード１１０に対応するクラス公開暗号鍵ＫＰｍ３によって、暗号化処理部５２１０によって暗号化される（ステップＳ３２０）。コントローラ５２２０は、バスＢＳ５を介して暗号化データ｛Ｋｓ２２｝Ｋｍ３を取得し、メモリ５２１５から取得したトランザクションＩＤを暗号化データ｛Ｋｓ２２｝Ｋｍ３に追加したトランザクションＩＤ／／｛Ｋｓ２２｝Ｋｍ３をバスＢＳ５、インタフェース５２２４および端子５２２６を介して出力する（ステップＳ３２２）。

【０３１２】図２７を参照して、パーソナルコンピュータ５０のコントローラ５１０は、バスＢＳ２を介してトランザクションＩＤ／／｛Ｋｓ２２｝Ｋｍ３を受信し（ステップＳ３２４）、ＵＳＢインタフェース５５０、端子５８０、およびＵＳＢケーブル７０を介してトランザクションＩＤ／／｛Ｋｓ２２｝Ｋｍ３を再生端末１００へ送信する（ステップＳ３２４）。そうすると、再生端末１００のコントローラ１１０６は、端子１１１４、ＵＳＢインタフェース１１１２、およびＢＳ３を介してトランザクションＩＤ／／｛Ｋｓ２２｝Ｋｍ３を受信し、その受信したトランザクションＩＤ／／｛Ｋｓ２２｝Ｋｍ３をメモリカードインタフェース１２００を介してメモリカード１１０へ送信する。そして、メモリカード１１０のコントローラ１４２０は、端子１４２６、インタフェース１４２４およびバスＢＳ４を介してトランザクションＩＤ／／｛Ｋｓ２２｝Ｋｍ３を受信する（ステップＳ３２６）。復号処理部１４２２は、コントローラ１４２０からバスＢＳ４を介して｛Ｋｓ２２｝Ｋｍ３を受取り、Ｋｍ保持部１４２１からのクラス秘密復号鍵Ｋｍ３によって｛Ｋｓ２２｝Ｋｍ３を復号してセッションキーＫｓ２２を受理する（ステップＳ３２８）。そして、セッションキー発生部１４１８は、セッションキーＫｓ２を生成し（ステップＳ３３０）、コントローラ１４２０は、バスＢＳ４を介してメモリ１４１５のＣＲＬ領域１４１５Ａから禁止クラスリストの更新日時ＣＲＬｄａｔｅを取得し、その取得した更新日時ＣＲＬｄａｔｅを切換スイッチ１４４６へ与える（ステップＳ３３２）。

【０３１３】そうすると、暗号化処理部１４０６は、切換スイッチ１４４６の端子を順次切換えることによって取得したセッションキーＫｓ２、個別公開暗号鍵ＫＰｍｃ４および更新日時ＣＲＬｄａｔｅを、復号処理部１４０４によって復号されたセッションキーＫｓ２２によって暗号化し、暗号化データ｛Ｋｓ２／／ＫＰｍｃ４／／ＣＲＬｄａｔｅ｝Ｋｓ２２を生成する。コントローラ１４２０は、暗号化データ｛Ｋｓ２／／ＫＰｍｃ４／／ＣＲＬｄａｔｅ｝Ｋｓ２２をバスＢＳ４、インタフェース１４２４および端子１４２６を介して再生端末１００へ出力し、再生端末１００のコントローラ１１０６は、メモリカードインタフェース１２００を介して暗号化データ｛Ｋｓ２／／ＫＰｍｃ４／／ＣＲＬｄａｔｅ｝Ｋｓ２２を受取る。そして、コントローラ１１０６は、ＵＳＢインタフェース１１１２、端子１１１４、およびＵＳＢケーブル７０を介してパーソナルコンピュータ５０へ送信する（ステップＳ３３４）。

【０３１４】パーソナルコンピュータ５０のコントローラ５１０は、端子５８０およびＵＳＢインタフェース５５０を介して暗号化データ｛Ｋｓ２／／ＫＰｍｃ４／／ＣＲＬｄａｔｅ｝Ｋｓ２２を受信し（ステップＳ３３６）、バスＢＳ２を介して暗号化データ｛Ｋｓ２／／ＫＰｍｃ４／／ＣＲＬｄａｔｅ｝Ｋｓ２２をライセンス管理デバイス５２０へ入力する（ステップＳ３３８）。ライセンス管理デバイス５２０のコントローラ５２２０は、端子５２２６、インタフェース５２２４およびバスＢＳ５を介して暗号化データ｛Ｋｓ２／／ＫＰｍｃ４／／ＣＲＬｄａｔｅ｝Ｋｓ２２を受信し、その受信した暗号化データ｛Ｋｓ２／／ＫＰｍｃ４／／ＣＲＬｄａｔｅ｝Ｋｓ２２を復号処理部５２１２に与える。復号処理部５２１２は、セッションキー発生部５２１８からのセッションキーＫｓ２２によって暗号化データ｛Ｋｓ２／／ＫＰｍｃ４／／ＣＲＬｄａｔｅ｝Ｋｓ２２を復号し、セッションキーＫｓ２、公開暗号鍵ＫＰｍｃ４および禁止クラスリストＣＲＬｄａｔｅを受理する（ステップＳ３４０）。

【０３１５】そうすると、パーソナルコンピュータ５０のコントローラ５１０は、ステップＳ３２４において、ライセンス管理ファイルに含まれるライセンスのエントリ番号をＨＤＤ５３０から読出す。そして、コントローラ５１０は、その読出したエントリ番号をバスＢＳ２を介してライセンス管理デバイス５２０に入力する（ステップＳ３４２）。ライセンス管理デバイス５２０のコントローラ５２２０は、端子５２２６、インタフェース５２２４、およびバスＢＳ５を介してエントリ番号を受信し、メモリ５２１５のライセンス領域５２１５Ｂにおいて受信したエントリ番号によって指定された領域からライセンス（トランザクションＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、アクセス制限情報ＡＣｍ、再生期限ＡＣｐ）を読出す（ステップＳ３４４）。

【０３１６】アクセス制限情報ＡＣｍの受理に応じて、コントローラ５２２０は、アクセス制限情報ＡＣｍを確認する（ステップＳ３４６）。つまり、コントローラ５２２０は、取得したアクセス制限情報ＡＣｍのセキュリティレベル、再生回数、移動複製フラグについて順に判定を行う。最初に、アクセス制限情報ＡＣｍのセキュリティレベルとステップＳ３１０にて用いた認証鍵に基づいて、レベル１認証鍵ＫＰａ１を利用し、かつ、アクセス制限情報ＡＣｍのセキュリティレベルが２の場合に

は、ライセンスの管理要求レベルより低いセキュリティレベルへ出力となるので、ステップＳ４０４へ移行し、移動動作を中止する。それ以外の場合には次の判定を行う。アクセス制限情報ＡＣｍの再生回数に基づいて、再生端末１００に装着されたメモリカード１１０へ移動しようとするライセンスがアクセス制限情報ＡＣｍによって暗号化コンテンツデータの再生ができないライセンスになっていないか否かを確認する。再生回数がアクセス制限情報ＡＣｍによる制限回数に達している場合（＝０）、暗号化コンテンツデータをライセンスによって再生することができず、その暗号化コンテンツデータとライセンスとを再生端末１００に装着されたメモリカード１１０へ移動する意味がないからである。再生回数が「０」の場合に、ステップＳ４０４へ移行し、移動動作を中止する。それ以外（再生回数≠０）の場合には次の判定を行う。アクセス制限情報ＡＣｍの移動複製フラグに基づいて、移動複製禁止「＝０」のときステップＳ４０４並行し、移動動作を中止する。移動のみ可のとき、ステップＳ３４８並行し、そして、コントローラ５２２０は、メモリ５２１５のライセンス領域５２１５Ｂにおいて指定されたエントリ番号内のライセンスを削除して（ステップＳ３４８」、ステップＳ３５０並行する。移動複製可「＝２」のとき、ライセンスの複製であると判断され、ステップＳ３４８を行なわずにステップＳ３５０並行。

【０３１７】図２８を参照して、暗号化処理部５２１７は、復号処理部５２１２によって得られたライセンス管理デバイス５２０固有の個別公開暗号鍵ＫＰｍｃ４によってライセンスを暗号化して暗号化データ｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４を生成する（ステップＳ３５０）。そして、メモリカード１１０から送信された更新日時ＣＲＬｄａｔｅをライセンス管理デバイス５２０がＣＲＬ領域５２１５Ａに保持している禁止クラスリストの更新日時と比較し、いずれの禁止クラスリストが新しいかが判断され、メモカード１００の方が新しいと判断されたとき、ステップＳ３５２へ移行する。また、ライセンス管理デバイス５２０の方が新しいと判断されたときはステップＳ３６２へ移行する（ステップＳ３５２）。

【０３１８】データＣＲＬｄａｔｅが最新と判断されたとき、暗号化処理部５２０６は、暗号化処理部５２１７から出力された暗号化データ｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４をセッションキー発生部５２１８において発生されたセッションキーＫｓ２によって暗号化を行い、暗号化データ｛｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２をバスＢＳ５に出力する。そして、コントローラ５２２０は、バスＢＳ５上の暗号化データ｛｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２をインタフェース５２２４および端子５２２６を介してパーソナルコンピュータ５０へ送信する（ステップＳ３５４）。

【０３１９】パーソナルコンピュータ５０のコントローラ５１０は、暗号化データ｛｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２を受取り、ＵＳＢインタフェース５５０、端子５８０、およびＵＳＢケーブル７０を介して再生端末１００へ送信する（ステップＳ３５６）。

【０３２０】再生端末１００のコントローラ１１０６は、端子１１１４、ＵＳＢインタフェース１１１２、およびバスＢＳ３を介して暗号化データ｛｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２を受信し、その受信した暗号化データ｛｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２をバスＢＳ３およびメモリカードインタフェース１２００を介してメモリカード１１０へ送信する。そして、メモリカード１１０のコントローラ１４２０は、端子１４２６、端子１４２４、およびバスＢＳ４を介して暗号化データ｛｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２を受信する（ステップＳ３５８）。

【０３２１】メモリカード１１０の復号処理部１４１２は、暗号化データ｛｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２をバスＢＳ４を介して受取り、セッションキー発生部１４１８によって発生されたセッションキーＫｓ２によって復号し、｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４を受理する（ステップＳ３６０）。その後、図２９に示すステップＳ３７６へ移行する。

【０３２２】一方、ステップＳ３５０において、ライセンス管理デバイス５２０の方が新しいと判断されると、ライセンス管理デバイス５２０のコントローラ５２２０は、バスＢＳ５を介してメモリ５２１５のＣＲＬ領域５２１５Ａから最新の禁止クラスリストＣＲＬを取得する（ステップＳ３６２）。

【０３２３】暗号化処理部５２０６は、暗号化処理部５２１７の出力と、コントローラ５２２０がバスＢＳ５を介してメモリ５２１５から取得した禁止クラスリストのデータＣＲＬとを、それぞれ、切換スイッチ５２４２および５２４６を介して受取り、セッションキー発生部５２１８において生成されたセッションキーＫｓ２によって暗号化する。暗号化処理部５２０６より出力された暗号化データ｛ＣＲＬ／／｛トランザクションＩＤ／／コンテンツＩＤ／インタフェース５２２４、および端子５２２６を介してパーソナルコンピュータ５０に出力される（ステップＳ３６４）。

【０３２４】パーソナルコンピュータ５０のコントロー

ラ５１０は、出力された暗号化データ｛ＣＲＬ／／｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２を受信し、ＵＳＢインタフェース５５０、端子５８０、およびＵＳＢケーブル７０を介して暗号化データ｛ＣＲＬ／／｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２を再生端末１００へ送信する（ステップＳ３６８）。再生端末１００のコントローラ１１０６は、端子１１１４、ＵＳＢインタフェース１１１２、およびバスＢＳ３を介して暗号化データ｛ＣＲＬ／／｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２を受取り、バスＢＳ３およびメモリカードインタフェース１２００を介して暗号化データ｛ＣＲＬ／／｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２をメモリカード１１０へ送信する。そして、メモリカード１１０のコントローラ１４２０は、端子１４２６、インタフェース１４２４、およびバスＢＳ４を介して暗号化データ｛ＣＲＬ／／｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２を受信する（ステップＳ３７０）。

【０３２５】メモリカード１１０において、復号処理部１４１２は、セッションキー発生部１４１８から与えられたセッションキーＫｓ２を用いてバスＢＳ４上の受信データを復号し、ＣＲＬと｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４とを受理する（ステップ３７２）。コントローラ１４２０は、復号処理部１４１２によって受理されたデータＣＲＬをバスＢＳ４を介して受取り、その受取ったデータＣＲＬによってメモリ１４１５のＣＲＬ領域１４１５Ａを書換える（ステップＳ３７４）。

【０３２６】ステップＳ３５４，Ｓ３５６，Ｓ３５８，Ｓ３６０は、送信側のメモリカード１１０の禁止クラスリストＣＲＬが、受信側のライセンス管理デバイス５２０の禁止クラスリストＣＲＬより、新しい場合のライセンス鍵Ｋｃ等のメモリカード１１０への移動動作であり、ステップＳ３６２，Ｓ３６４，Ｓ３６８，Ｓ３７０，Ｓ３７２，Ｓ３７４は、送信側のライセンス管理デバイス５２０の禁止クラスリストＣＲＬが、受信側のメモリカード１１０の禁止クラスリストＣＲＬより、新しい場合のライセンス鍵Ｋｃ等のメモリカード１１０への移動動作である。このように、メモリカード１１０から送られてきた禁止クラスリストの更新日時ＣＲＬｄａｔｅによって、逐一、確認し、より最新の禁止クラスリストＣＲＬをメモリカード１１０の禁止クラスリストＣＲＬとしてＣＲＬ領域１５１４Ａに格納させることによって、クラス秘密鍵が漏洩などのセキュリティ機能の破られた機器へのライセンスの流出をを防止できる。

【０３２７】図２９を参照して、ステップＳ３６０またはステップＳ３７４の後、コントローラ１４２０の指示によって、暗号化ライセンス｛トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４は、復号処理部１４０４において、個別秘密復号鍵Ｋｍｃ４によって復号され、ライセンス（ライセンス鍵Ｋｃ、トランザクションＩＤ、コンテンツＩＤ、アクセス制限情報ＡＣｍおよび再生期限ＡＣｐ）が受理される（ステップＳ３７６）。

【０３２８】このように、ライセンス管理デバイスおよびメモリカードでそれぞれ生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、暗号化コンテンツデータおよびライセンスの移動動作におけるセキュリティを向上させることができる。

【０３２９】パーソナルコンピュータ５０のコントローラ５１０は、メモリカード１１０へ移動したライセンスを格納するためのエントリ番号を、ＵＳＢインタフェース５５０、端子５８０、およびＵＳＢケーブル７０を介して再生端末１００へ送信する（ステップＳ３７８）。そうすると、再生端末１００のコントローラ１１０６は、端子１１１４、ＵＳＢインタフェース１１１２、およびバスＢＳ３を介してエントリ番号を受取り、バスＢＳ３およびメモリカードインタフェース１２００を介してメモリカード１１０へ送信し、メモリカード１１０のコントローラ１４２０は、端子１４２６およびインタフェース１４２４を介してエントリ番号を受取り、その受取ったエントリ番号によって指定されるメモリ１４１５のライセンス領域１４１５Ｂに、ステップＳ３７６において取得したライセンス（ライセンス鍵Ｋｃ、トランザクションＩＤ、コンテンツＩＤ、アクセス制限情報ＡＣｍおよび再生期限ＡＣｐ）を格納する（ステップＳ３８０）。

【０３３０】パーソナルコンピュータ５０のコントローラ５１０は、メモリカード１１０のメモリ１４１５に格納されたライセンスのエントリ番号と、平文のトランザクションＩＤおよびコンテンツＩＤを含むメモリカード１１０へ移動しようとする暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆに対するライセンス管理ファイルを生成し、メモリカード１１０へ送信する（ステップＳ３８２）。

【０３３１】メモリカード１１０のコントローラ１４２０は、再生端末１００を介してライセンス管理ファイルを受信し、メモリ１４１５のデータ領域１４１５Ｃに受信したライセンス管理ファイルを記録する（ステップＳ３８４）。

【０３３２】そして、パーソナルコンピュータ５０のコントローラ５１０は、ステップＳ３４６の判断に従って、移動であればステップＳ３８８へ移行し、複製であ

ればステップS388を行なわないで、ステップS390並行する(ステップS386)。そして、移動の場合、HDD530に記録されたライセンスのうち、メモリカード110へ移動したライセンスに対するライセンス管理ファイルのライセンスエントリ番号を、ライセンス無に更新する(ステップS386)。

【0333】その後、コントローラ510は、メモリカード110へ移動しようとするコンテンツファイル(暗号化コンテンツデータ{Dc}Kcと付加情報Dc-inf)とをHDD530から取得し、{Dc}Kc//Dc-infをメモリカード110へ送信する(ステップS390)。メモリカード110のコントローラ1420は、再生端末100を介して{Dc}Kc//Dc-infを受信し(ステップS392)、バスBS4を介して受信した{Dc}Kc//Dc-infをコンテンツファイルとしてメモリ1415のデータ領域1415Cに記録する(ステップS394)。

【0334】そうすると、パーソナルコンピュータ50のコントローラ510は、メモリカード110へ移動した楽曲を追記した再生リストファイルを作成し(ステップS396)、再生リストファイルと、再生リストファイルの書換指示とをメモリカード110へ送信する(ステップS398)。メモリカード110のコントローラ1420は、再生端末100を介して再生リストファイルと書換指示とを受信し(ステップS400)、バスBS4を介してメモリ1415のデータ領域1415Cに記録されている再生リストファイルを受信した再生リストファイルに書換え(ステップS402)、移動動作が終了する(ステップS404)。

【0335】なお、再生リストファイルとは、HDDに記録されていたコンテンツリストファイルと、同じ目的で作られた再生端末用の管理情報ファイルである。再生端末100は、この再生リストファイルに含まれるコンテンツの登場順に、コンテンツファイルおよびライセンス管理ファイルを特定して再生を行なう。

【0336】このようにして、再生端末100に装着されたメモリカード110が正規の機器であること、同時に、クラス証明書Cm3とともに暗号化して送信できた公開暗号鍵KPm3が有効であることを確認した上で、クラス証明書Cm3が禁止クラスリスト、すなわち、公開暗号鍵KPm3による暗号化が破られたクラス証明書リストに記載されていないメモリカードへの移動要求に対してのみコンテンツデータを移動することができ、不正なメモリカードへの移動および解読されたクラス鍵を用いた移動を禁止することができる。また、この移動動作を用いることによって、配信サーバ10との通信機能を有さない再生端末102のユーザも、パーソナルコンピュータ50を介して暗号化コンテンツデータおよびライセンスをメモリカードに受信することができ、ユーザの利便性は向上する。

【0337】また、説明から明らかなように移動処理として説明したが、コンテンツ供給者によって、ライセンスの複製が許可されている場合には、複製処理として実行され、送信側のライセンス管理デバイス511にライセンスはそのまま保持される。この場合の複製は、配信時にコンテンツ供給者、すなわち、著作権所有者が複製を許可し、アクセス制限情報ACmの移動複製フラグを移動複製可に設定した場合にのみ許可される行為で合え居、著作権所有者の権利を阻害した行為ではない。アクセス制限情報はライセンスの一部であり、その機密性は保証されているにで、著作権は保護されている。

【0338】なお、上記においては、パーソナルコンピュータ50のライセンス管理デバイス520からメモリカード110へのライセンスの移動について説明したが、メモリカード110からライセンス管理デバイス520へのライセンスの移動も、図26～図29に示すフローチャートに従って行なわれる。また、パーソナルコンピュータ50が配信サーバ10から受信した暗号化コンテンツデータおよびライセンスをメモリカード110へ移動できるのでは、ライセンス管理デバイス520が配信サーバ10からハード的に受信した暗号化コンテンツデータおよびライセンスだけであり、ライセンス管理モジュール511が配信サーバ10からソフト的に受信した暗号化コンテンツデータおよびライセンスを「移動」という概念によってメモリカードへ送信することはできない。ライセンス管理モジュール511は、ライセンス管理デバイス520よりも低いセキュリティレベルによってソフト的に配信サーバ10との間で認証データおよび暗号鍵等のやり取りを行ない、暗号化コンテンツデータおよびライセンスを受信するので、その受信動作において暗号化が破られる可能性は、ライセンス管理デバイス520によって暗号化コンテンツデータおよびライセンスを受信する場合よりも高い。したがって、低いセキュリティレベルによって受信し、かつ、管理された暗号化コンテンツデータおよびライセンスを、ライセンス管理デバイス520と同じセキュリティレベルによって暗号化コンテンツデータおよびライセンスを受信して管理するメモリカード110へ「移動」という概念によって自由に移すことができるとすると、メモリカード110におけるセキュリティレベルが低下するので、これを防止するためにライセンス管理モジュール511によって受信した暗号化コンテンツデータおよびライセンスを「移動」という概念によってメモリカード110へ送信できなくしたものである。

【0339】しかしながら、ライセンス管理モジュール511によって受信されたセキュリティレベルの低い暗号化コンテンツデータおよびライセンスを、一切、メモリカード110へ移すことができないとすると、著作権を保護しながらコンテンツデータの自由なコピーを許容するデータ配信システムの趣旨に反し、ユーザの利便性

も向上しない。そこで、次に説明するチェックアウトおよびチェックインの概念によってライセンス管理モジュール５１１によって受信した暗号化コンテンツデータおよびライセンスをメモリカード１１０へ送信できるようにした。

【０３４０】[チェックアウト]図１に示すデータ配信システムにおいて、配信サーバ１０からパーソナルコンピュータ５０のライセンス管理モジュール５１１へ配信された暗号化コンテンツデータおよびライセンスを再生端末１００に装着されたメモリカード１１０に送信する動作について説明する。なお、この動作を「チェックアウト」という。

【０３４１】図３０～図３４は、図１に示すデータ配信システムにおいて、ライセンス管理モジュール５１１が配信サーバ１０から受信した暗号化コンテンツデータおよびライセンスを、返却を条件として再生端末１００に装着されたメモリカード１１０へ貸出すチェックアウト動作を説明するための第１～第５のフローチャートである。なお、図３０における処理以前に、パーソナルコンピュータ５０のユーザは、コンテンツリストファイルに従って、チェックアウトするコンテンツを決定し、ＨＤＤ５３０のコンテンツファイルおよびライセンス管理ファイルが特定でき、メモリカード１１０の再生リストファイルを取得してていることを前提として説明する。

【０３４２】図３０を参照して、パーソナルコンピュータ５０のキーボード５６０からチェックアウトリクエストが入力されると（ステップＳ５００）、ライセンス管理モジュール５１１は、バインディング鍵取得処理を行う。図３０のステップＳ５０１から図３１のステップＳ５１５の一連の処理がバインディング鍵取得処理であり、配信２のフローチャートにおける図２０のステップＳ２７０から図２１のステップＳ２８４の一連の処理と同じである。ゆえに、説明を省略する。

【０３４３】バインディング鍵Ｋｂを取得したライセンス管理モジュール５１１は、バスＢＳ２を介してＨＤＤ５３０から暗号化機密ファイル１６０を取得し、その取得した暗号化機密ファイル１６０をバインディング鍵Ｋｂによって復号して平文の機密ファイルを取得する（ステップＳ５１６）。その後、ライセンス管理モジュール５１１は、ライセンス管理ファイルに記録された機密情報番号ｎに対応する機密ファイル内の機密情報ｎ（トランザクションＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、アクセス制限情報ＡＣｍ、再生期限ＡＣｐ、およびチェックアウト情報）を取得する（ステップＳ５１７）。

【０３４４】そうすると、ライセンス管理モジュール５１１は、取得したアクセス制限情報ＡＣｍに基づいてライセンスがチェックアウト可能か否かを確認する（ステップＳ５１８）、つまり、ライセンス管理モジュール５１１は、再生端末１００に装着されたメモリカード１１０へチェックアウトしようとするライセンスがアクセス制限情報ＡＣｍの再生回数によって暗号化コンテンツデータの再生回数の制限がないか、再生ができないライセンスになっていないか否かを確認する。再生回数に制限がある場合、暗号化コンテンツデータおよびライセンスをチェックアウトしない。

【０３４５】ステップＳ５１８において、再生に制限がある場合、ステップＳ５６４へ移行し、チェックアウト動作は終了する。ステップＳ５１８において、暗号化コンテンツデータの再生回数がアクセス制限情報ＡＣｍによる制限回数に達していない場合、ステップＳ５１９へ移行する。そして、ライセンス管理モジュール５１１は、取得したチェックアウト情報に含まれるチェックアウト可能数が「０」よりも大きいか否かを確認する（ステップＳ５１９）。ステップＳ５１９において、チェックアウト可能数が「０」であれば、チェックアウトできるライセンスが無いので、ステップＳ５６４へ移行し、チェックアウト動作は終了する。ステップＳ５１９において、チェックアウト可能数が「０」よりも大きいとき、ライセンス管理モジュール５１１は、ＵＳＢインタフェース５５０、端子５８０、およびＵＳＢケーブル７０を介して認証データの送信要求を送信する（ステップＳ５２０）。再生端末１００のコントローラ１１０６は、端子１１１４、ＵＳＢインタフェース１１１２、およびバスＢＳ３を介して認証データの送信要求を受信し、その受信した認証データの送信要求をバスＢＳ３およびメモリカードインタフェース１２００を介してメモリカード１１０へ送信する。そして、メモリカード１１０のコントローラ１４２０は、端子１４２６、インタフェース１４２４およびバスＢＳ４を介して認証データの送信要求を受信する（ステップＳ５２１）。

【０３４６】コントローラ１４２０は、認証データの送信要求を受信すると、認証データ保持部１４００から認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａ２をバスＢＳ４を介して読出し、その読出した認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａ２をバスＢＳ４、インタフェース１４２４および端子１４２６を介して再生端末１００へ出力する。そして、再生端末１００のコントローラ１１０６は、メモリカードインタフェース１２００およびバスＢＳ３を介して認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａ２を受取り、バスＢＳ３、ＵＳＢインタフェース１１１２、端子１１１４およびＵＳＢケーブル７０を介してパーソナルコンピュータ５０へ認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａ２を送信する（ステップＳ５２２）。

【０３４７】そうすると、パーソナルコンピュータ５０のライセンス管理モジュール５１１は、端子５８０およびＵＳＢインタフェース５５０を介して認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａ２を受信し（ステップＳ５２３）、その受信した認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａ２をレベル２認証鍵ＫＰａ２によって復号する

（ステップＳ５２４）。

【０３４８】図３２を参照して、ライセンス管理モジュール５１１は、復号処理結果から、処理が正常に行なわれたか否か、すなわち、メモリカード１１０が正規のメモリカードからのクラス公開暗号鍵ＫＰｍ３とクラス証明書Ｃｍ３とを保持することを認証するために、正規の機関でその正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行なう（ステップＳ５２５）。正当な認証データであると判断された場合、ライセンス管理モジュール５１１は、クラス公開暗号鍵ＫＰｍ３およびクラス証明書Ｃｍ３を承認し、受理する。そして、次の処理（ステップＳ５２６）へ移行する。正当な認証データでない場合には、非承認とし、クラス公開暗号鍵ＫＰｍ３およびクラス証明書Ｃｍ３を受理しないで処理を終了する（ステップＳ５６４）。

【０３４９】認証の結果、正規のメモリカードであることが認識されると、ライセンス管理モジュール５１１は、次に、メモリカード１１０のクラス証明書Ｃｍ３が禁止クラスリストＣＲＬにリストアップされているかどうかをＨＤＤ５３０に照会し、これらのクラス証明書が禁止クラスリストの対象になっている場合には、ここでチェックアウト動作を終了する（ステップＳ５６４）。一方、メモリカード１１０のクラス証明書が禁止クラスリストの対象外である場合には次の処理に移行する（ステップＳ５２６）。

【０３５０】認証の結果、正当な認証データを持つメモリカードを備える再生端末からのアクセスであり、クラスが禁止クラスリストの対象外であることが確認されると、ライセンス管理モジュール５１１は、チェックアウトを特定するための管理コードであるチェックアウト用トランザクションＩＤを、メモリカード１１０の格納されている全てのトランザクションＩＤと異なる値をとり、かつ、ローカル使用のトランザクションＩＤとして生成する。生成する（ステップＳ５２７）。そして、ライセンス管理モジュール５１１は、チェックアウトのためのセッションキーＫｓ２ｂを生成し（ステップＳ５２８）、メモリカード１１０から送信されたクラス公開暗号鍵ＫＰｍ３によって、生成したセッションキーＫｓ２ｂを暗号化する（ステップＳ５２９）。そして、ライセンス管理モジュール５１１は、暗号化データ｛Ｋｓ２ｂ｝Ｋｍ３にチェックアウト用トランザクションＩＤを追加したチェックアウト用トランザクションＩＤ／／｛Ｋｓ２ｂ｝Ｋｍ３をＵＳＢインタフェース５５０、端子５８０、およびＵＳＢケーブル７０を介して再生端末１００へ送信する（ステップＳ５３０）。そうすると、再生端末１００のコントローラ１１０６は、端子１１１４、ＵＳＢインタフェース１１１２、およびバスＢＳ３を介してチェックアウト用トランザクションＩＤ／／｛Ｋｓ２ｂ｝Ｋｍ３を受信し、その受信したチェックアウト用トランザクションＩＤ／／｛Ｋｓ２ｂ｝Ｋｍ３をメモリカードインタフェース１２００を介してメモリカード１１０へ送信する。そして、メモリカード１１０のコントローラ１４２０は、端子１４２６、インタフェース１４２４およびバスＢＳ４を介してチェックアウト用トランザクションＩＤ／／｛Ｋｓ２ｂ｝Ｋｍ３を受信する（ステップＳ５３１）。復号処理部１４２２は、コントローラ１４２０からバスＢＳ４を介して｛Ｋｓ２ｂ｝Ｋｍ３を受取り、Ｋｍ保持部１４２１からの秘密復号鍵Ｋｍ３によって｛Ｋｓ２ｂ｝Ｋｍ３を復号してセッションキーＫｓ２ｂを受理する（ステップＳ５３２）。そして、セッションキー発生部１４１８は、セッションキーＫｓ２ｃを生成し（ステップＳ５３３）、コントローラ１４２０は、バスＢＳ４を介してメモリ１４１５のＣＲＬ領域１４１５Ａから禁止クラスリストの更新日時ＣＲＬｄａｔｅを取得し、その取得した更新日時ＣＲＬｄａｔｅを切換スイッチ１４４６へ与える（ステップＳ５３４）。

【０３５１】そうすると、暗号化処理部１４０６は、切換スイッチ１４４６の端子を順次切換えることによって取得したセッションキーＫｓ２ｃ、個別公開暗号鍵ＫＰｍｃ４および更新日時ＣＲＬｄａｔｅを、復号処理部１４０４によって復号されたセッションキーＫｓ２ｂによって暗号化し、暗号化データ｛Ｋｓ２ｃ／／ＫＰｍｃ４／／ＣＲＬｄａｔｅ｝Ｋｓ２ｂを生成する。コントローラ１４２０は、暗号化データ｛Ｋｓ２ｃ／／ＫＰｍｃ４／／ＣＲＬｄａｔｅ｝Ｋｓ２ｂをバスＢＳ４、インタフェース１４２４および端子１４２６を介して再生端末１００へ出力し、再生端末１００のコントローラ１１０６は、メモリカードインタフェース１２００を介して暗号化データ｛Ｋｓ２ｃ／／ＫＰｍｃ４／／ＣＲＬｄａｔｅ｝Ｋｓ２ｂを受取る。そして、コントローラ１１０６は、ＵＳＢインタフェース１１１２、端子１１１４、およびＵＳＢケーブル７０を介してパーソナルコンピュータ５０へ送信する（ステップＳ５３５）。

【０３５２】パーソナルコンピュータ５０のライセンス管理モジュール５１１は、端子５８０およびＵＳＢインタフェース５５０を介して暗号化データ｛Ｋｓ２ｃ／／ＫＰｍｃ４／／ＣＲＬｄａｔｅ｝Ｋｓ２ｂを受信し（ステップＳ５３６）、その受信した暗号化データ｛Ｋｓ２ｃ／／ＫＰｍｃ４／／ＣＲＬｄａｔｅ｝Ｋｓ２ｂをセッションキーＫｓ２ｂによって復号し、セッションキーＫｓ２ｃ、個別公開暗号鍵ＫＰｍｃ４および更新日時ＣＲＬｄａｔｅを受理する（ステップＳ５３７）。そして、ライセンス管理モジュール５１１は、再生端末１００に装着されたメモリカードから他のメモリカード等へライセンスが移動／複製されるのを禁止したチェックアウト用アクセス制限情報ＡＣｍを生成する。すなわち、再生回数を無制限（＝２５５）、移動複製フラグを移動複製不可（＝３）、セキュリティレベルを１に設定したアク

セス制限情報ＡＣｍを生成する（ステップＳ５３８）。

【０３５３】図３３を参照して、ライセンス管理モジュール５１１は、ステップＳ５３７において受信したメモリカード１１０に固有の公開暗号鍵ＫＰｍｃ４によってライセンスを暗号化して暗号化データ｛チェックアウト用トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／チェックアウト用ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４を生成する（ステップＳ５３９）。そして、メモリカード１１０から送信された更新日時ＣＲＬｄａｔｅが、ライセンス管理モジュール５１１が管理するＨＤＤ５３０に保持される禁止クラスリストの更新日時と比較し、いずれの禁止クラスリストが新しいかが判断され、メモリカード１１０の方が新しいと判断されたとき、ステップＳ５４１へ移行する。また、逆に、ライセンス管理モジュール５１１の方が新しいと判断されたときはステップＳ５４４へ移行する（ステップＳ５４０）。

【０３５４】メモリカード１１０の方が新しいと判断されたとき、ライセンス管理モジュール５１１は、暗号化データ｛チェックアウト用トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／チェックアウト用ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４をセッションキーＫｓ２ｃによって暗号化を行い、暗号化データ｛｛チェックアウト用トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／チェックアウト用ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２ｃをＵＳＢインタフェース５５０、端子５８０、およびＵＳＢケーブル７０を介して再生端末１００へ送信する（ステップＳ５４１）。

【０３５５】再生端末１００のコントローラ１１０６は、端子１１１４、ＵＳＢインタフェース１１１２、およびバスＢＳ３を介して暗号化データ｛｛チェックアウト用トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／チェックアウト用ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２ｃを受信し、その受信した暗号化データ｛｛チェックアウト用トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／チェックアウト用ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２ｃをバスＢＳ３およびメモリカードインタフェース１２００を介してメモリカード１１０へ送信する。そして、メモリカード１１０のコントローラ１４２０は、端子１４２６、端子１４２４、およびバスＢＳ４を介して暗号化データ｛｛チェックアウト用トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／チェックアウト用ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２ｃを受信する（ステップＳ５４２）。

【０３５６】メモリカード１１０の復号処理部１４１２は、暗号化データ｛｛チェックアウト用トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／チェックアウト用ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２ｃをバスＢＳ４を介して受取り、セッションキー発生部１４１８によって発生されたセッションキーＫｓ２ｃによって復号し、｛チェックアウト用トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／チェックアウト用ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４を受理する（ステップＳ５４３）。その後、図３４に示すステップＳ５４９へ移行する。

【０３５７】一方、ステップＳ５４０において、ライセンス管理モジュール５１１の禁止クラスリストのほうが新しいと判断されると、ライセンス管理モジュール５１１は、ＨＤＤ５３０からライセンス管理モジュール５１１の管理する禁止クラスリストＣＲＬを取得する（ステップＳ５４４）。

【０３５８】そして、ライセンス管理モジュール５１１は、｛チェックアウト用トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／チェックアウト用ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４と、ＨＤＤ５３０から取得した禁止クラスリストのデータＣＲＬとをセッションキーＫｓ２ｃによって暗号化し、その暗号化データ｛ＣＲＬ／／｛チェックアウト用トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／チェックアウト用ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２ｃをＵＳＢインタフェース５５０、端子５８０およびＵＳＢケーブル７０を介して再生端末１００へ送信する（ステップＳ５４５）。再生端末１００のコントローラ１１０６は、端子１１１４、ＵＳＢインタフェース１１１２、およびバスＢＳ３を介して暗号化データ｛ＣＲＬ／／｛チェックアウト用トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／チェックアウト用ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２ｃを受信し、その受信した暗号化データ｛ＣＲＬ／／｛チェックアウト用トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／チェックアウト用ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２ｃをバスＢＳ３およびメモリカードインタフェース１２００を介してメモリカード１１０へ出力する。そうすると、メモリカード１１０のコントローラ１４２０は、端子１４２６、インタフェース１４２４、およびバスＢＳ４を介して暗号化データ｛ＣＲＬ／／｛チェックアウト用トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／チェックアウト用ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２ｃを受信する（ステップＳ５４６）。

【０３５９】メモリカード１１０において、復号処理部１４１２は、セッションキー発生部１４１８から与えられたセッションキーＫｓ２ｃを用いてバスＢＳ４上の受信データを復号し、ＣＲＬと｛チェックアウト用トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／チェックアウト用ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４とを受理する（ステップ５４７）。コントローラ１４２０は、復号処理部１４１２によって受理されたデータＣＲＬをバスＢＳ４を介して受取り、その受取ったデータＣＲＬによってメモリ１４１５のＣＲＬ領域１４１５Ａを書換える（ステップＳ５４８）。

【０３６０】ステップＳ５４１，Ｓ５４２，Ｓ５４３は、送信側のライセンス管理モジュール５１１の禁止クラスリストＣＲＬより、受信側のメモリカード１１０の

禁止クラスリストＣＲＬが新しい場合のライセンス鍵Ｋｃ等のメモリカード１１０へのチェックアウト動作であり、ステップＳ５４４，Ｓ５４５，Ｓ５４６，Ｓ５４７，Ｓ５４８は、受信側のメモリカード１１０の禁止クラスリストＣＲＬより、送信側のライセンス管理モジュール５１１の禁止クラスリストＣＲＬが新しい場合のライセンス鍵Ｋｃ等のメモリカード１１０へのチェックアウト動作である。このように、メモリカード１１０へライセンスを送信するときに、メモリカード１００がＣＲＬ領域１４１５Ｂで保持する禁止クラスリストＣＲＬより、ＨＤＤ５３０に新しい禁止クラスリストＣＲＬが記録されている場合には禁止クラスリストＣＲＬをＨＤＤ５３０から取得し、禁止クラスリストＣＲＬをメモリカード１１０に配信することによって、メモリカード１００がＣＲＬ領域１４１５Ｂで保持する禁止クラスリストを更新していくことができる、クラス鍵が破られたメモリカード１１０へのらい線への送信を禁止することができ、配信されたライセンスの流出を防止できる。

【０３６１】図３４を参照して、ステップＳ５４３またはステップＳ５４８の後、コントローラ１４２０の指示によって、暗号化ライセンス｛チェックアウト用トランザクションＩＤ／／コンテンツＩＤ／／Ｋｃ／／チェックアウト用ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４は、復号処理部１４０４において、秘密復号鍵Ｋｍｃ４によって復号され、ライセンス（ライセンス鍵Ｋｃ、チェックアウト用トランザクションＩＤ、コンテンツＩＤ、チェックアウト用ＡＣｍおよび再生期限ＡＣｐ）が受理される（ステップＳ５４９）。

【０３６２】そして、パーソナルコンピュータ５０のライセンス管理モジュール５１１は、メモリカード１１０へチェックアウトしたライセンスを格納するためのエントリ番号を、ＵＳＢインタフェース５５０、端子５８０、およびＵＳＢケーブル７０を介して再生端末１０２へ送信しする（ステップＳ５５０）。そうすると、再生端末１０２のコントローラ１１０６は、端子１１１４、ＵＳＢインタフェース１１１２、およびバスＢＳ３を介してエントリ番号を受取り、その受取ったエントリ番号によって指定されるメモリ１４１５のライセンス領域１４１５Ｂに、ステップＳ５６６において受理したライセンス（ライセンス鍵Ｋｃ、チェックアウト用トランザクションＩＤ、コンテンツＩＤ、チェックアウト用ＡＣｍおよび再生制御情報ＡＣｐ）を格納する（ステップＳ５５１）。

【０３６３】パーソナルコンピュータ５０のライセンス管理モジュール５１１は、メモリカード１１０のメモリ１４１５に格納されたライセンスのエントリ番号と、平文のチェックアウト用トランザクションＩＤおよびコンテンツＩＤを含むメモリカード１１０へ移動しようとする暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆに対するライセンス管理ファイルを生成し、メモリカード１１０へ送信する（ステップＳ５５２）。

【０３６４】メモリカード１１０のコントローラ１４２０は、再生端末１０２を介してライセンス管理ファイルを受信し、メモリ１４１５のデータ領域１４１５Ｃに受信したライセンス管理ファイルを記録する（ステップＳ５５３）。

【０３６５】パーソナルコンピュータ５０のライセンス管理モジュール５１１は、チェックアウト可能数を１減算し、チェックアウト用トランザクションＩＤとチェックアウト先のメモリカードに固有の公開暗号鍵ＫＰｍｃ４とを追加してチェックアウト情報を更新する（ステップＳ５５４）。そして、ライセンス管理モジュール５１１は、トランザクションＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、アクセス制限情報ＡＣｍ、再生期限ＡＣｐ、および更新したアドレス情報（チェックアウト可能数と、チェックアウト用トランザクションＩＤと、チェックアウト先のメモリカード１１０に個別の戸別公開暗号鍵ＫＰｍｃ４を追加したもの）を新たな機密情報ｎとして平文の機密ファイルを更新する（ステップＳ５５５）。チェックアウト先の個別公開鍵ＫＰｍｃ４は、個別公開鍵はメモリカードの耐タンパモジュール無いに格納され、かつ、認証による暗号を用いたセキュリティの高い通信手段によって入手するメモリカードごとに固有値を持つため、メモリカード特定する識別情報として適している。

【０３６６】その後、ライセンス管理モジュール５１１は、平文の機密ファイルをバインディング鍵Ｋｂによって暗号化してＨＤＤ５３０に記録されている暗号化機密ファイル１６０を更新する（ステップＳ５５６）。

【０３６７】ライセンス管理モジュール５１１は、メモリカード１１０へチェックアウトしようとする暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆとをＨＤＤ５３０から取得し、｛Ｄｃ｝Ｋｃ／／Ｄｃ－ｉｎｆをメモリカード１１０へ送信する（ステップＳ５５７）。メモリカード１１０のコントローラ１４２０は、再生端末１００を介して｛Ｄｃ｝Ｋｃ／／Ｄｃ－ｉｎｆを受信し（ステップＳ５５８）、バスＢＳ４を介して受信した｛Ｄｃ｝Ｋｃ／／Ｄｃ－ｉｎｆをメモリ１４１５のデータ領域１４１５Ｃに記録する（ステップＳ５５９）。

【０３６８】そうすると、パーソナルコンピュータ５０のライセンス管理モジュール５１１は、メモリカード１１０へチェックアウトした楽曲を追記した再生リストファイルを作成し（ステップＳ５６０）、再生リストファイルと、再生リストファイルとの書換指示とをメモリカード１１０へ送信する（ステップＳ５６１）。メモリカード１１０のコントローラ１４２０は、再生端末１００を介して再生リストと書換指示とを受信し（ステップＳ５６２）、バスＢＳ４を介してメモリ１４１５のデータ領域１４１５Ｃに記録されている再生リストファイルを

受信した再生リストファイルに書換え（ステップS563）、チェックアウト動作が終了する（ステップS564）。

【0369】このようにして、再生端末100に装着されたメモリカード110が正規の機器であること、同時に、クラス証明書Cm3とともに暗号化して送信されたクラス公開暗号鍵KPm3が有効であることを確認した上で、クラス証明書Cm3が禁止クラスリスト、すなわち、クラス公開暗号鍵KPm3による暗号化が破られたクラス証明書リストに記載されていないメモリカードへのチェックアウト要求に対してのみコンテンツデータをチェックアウトすることができ、不正なメモリカードへのチェックアウトおよび解読されたクラス鍵を用いたチェックアウトを禁止することができる。また、ライセンス管理モジュールおよびメモリカードでそれぞれ生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、暗号化コンテンツデータおよびライセンスのチェックアウト動作におけるセキュリティを向上させることができる。さらに、このチェックアウト動作を用いることによって、配信サーバ10との通信機能を有さない再生端末100のユーザも、パーソナルコンピュータ50がソフトウエアによって受信した暗号化コンテンツデータおよびライセンスをメモリカードに受信することができ、ユーザの利便性は向上する。

【0370】［チェックイン］図1に示すデータ配信システムにおいて、パーソナルコンピュータ50のライセンス管理モジュール511からメモリカード110へチェックアウトされた暗号化コンテンツデータおよびライセンスをライセンス管理モジュール511へ戻す動作について説明する。なお、この動作を「チェックイン」という。

【0371】図35～図38は、図30～図34を参照して説明したチェックアウト動作によってメモリカード110へ貸出された暗号化コンテンツデータおよびライセンスを返却して貰うチェックイン動作を説明するための第1～第4のフローチャートである。なお、図35における処理以前に、パーソナルコンピュータ50のユーザは、HDD520に記録されているコンテンツリストファイルとメモリカード110のデータ領域1415Bに記録されている再生リストファイルを取得し、両ファイルに従って、チェックインするコンテンツを決定し、HDD530およびメモカード110のコンテンツファイルおよびライセンス管理ファイルが特定でき、かつ、メモリカード110のライセンス管理ファイルを取得してていることを前提として説明する。

【0372】図35を参照して、パーソナルコンピュータ50のキーボード560からチェックインリクエストが入力されると（ステップS600）、ライセンス管理モジュール511は、バインディング鍵取得処理を行う。図35のステップS601から図36のステップ615の一連の処理がバインディング鍵取得処理であり、配信2のフローチャートにおける図20のステップS270から図21のステップS284の一連の処理と同じである。ゆえに、説明を省略する。

【0373】バインディング鍵Kbを取得したライセンス管理モジュール511は、バスBS2を介してHDD530から暗号化機密ファイル160を取得し、その取得した暗号化機密ファイル160をバインディング鍵Kbによって復号して平文の機密ファイルを取得する（ステップS616）。その後、ライセンス管理モジュール511は、ライセンス管理ファイルに記録された機密情報番号nに対応する機密ファイル内の機密情報n（ライセンス（トランザクションID、コンテンツID、ライセンス鍵Kc、アクセス制限情報ACm、再生期限ACp）、およびチェックアウト情報（チェックアウト可能数、チェックアウト用トランザクションID、チェックアウト先のメモリカードの個別公開暗号鍵KPmcx））を取得する（ステップS617）。そして、ライセンス管理モジュール511は、認証データの送信要求をUSBインターフェース550、端子580、およびUSBケーブル70を介して再生端末100へ送信する（ステップS618）。

【0374】そうすると、再生端末100のコントローラ1106は、端子1114、USBインタフェース1112およびバスBS3を介して認証データの送信要求を受信し、バスBS3およびメモリカードインタフェース1200を介して認証データの送信要求をメモリカード110へ送信する。そして、メモリカード110のコントローラ1420は、端子1426、インタフェース1424およびバスBS4を介して認証データの送信要求を受信する（ステップS619）。

【0375】コントローラ1420は、認証データの送信要求を受信すると、認証データ保持部1400から認証データ｛KPm3／／Cm3｝KPa2をバスBS4を介して読出し、その読出した認証データ｛KPm3／／Cm3｝KPa2をバスBS4、インタフェース1424および端子1426を介して再生端末100へ出力する。そして、再生端末100のコントローラ1106は、メモリカードインタフェース1200およびバスBS3を介して認証データ｛KPm3／／Cm3｝KPa2を受取り、バスBS3、USBインタフェース1112、端子1114およびUSBケーブル70を介してパーソナルコンピュータ50へ認証データ｛KPm3／／Cm3｝KPa2を送信する（ステップS620）。

【0376】パーソナルコンピュータ50のライセンス管理モジュール511は、端子580およびUSBインタフェース550を介して認証データ｛KPm3／／C

m3}KPa2を受信し（ステップS621）、その受信した認証データ{KPm3//Cm3}KPa2をレベル2認証鍵KPaによって復号する（ステップS622）。そして、ライセンス管理モジュール511は、復号処理結果から、処理が正常に行なわれたか否か、すなわち、メモリカード110が正規のメモリカードからのクラス公開暗号鍵KPm3とクラス証明書Cm3とを保持することを認証するために、正規の機関でその正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行なう（ステップS623）。正当な認証データであると判断された場合、ライセンス管理モジュール511は、クラス公開暗号鍵KPm3およびクラス証明書Cm3を承認し、受理する。そして、次の処理（ステップS624）へ移行する。正当な認証データでない場合には、非承認とし、クラス公開暗号鍵KPm3およびクラス証明書Cm3を受理しないで処理を終了する（ステップS653）。認証の結果、正規のメモリカードであることが認識されると、ライセンス管理モジュール511は、ダミートランザクションIDを生成する（ステップS624）。ダミー用トランザクションIDは、必ず、メモリカード110の格納されている全てのトランザクションIDと異なる値をとり、かつ、ローカル使用のトランザクションIDとして生成する。

【0377】図37を参照して、ライセンス管理モジュール511は、チェックイン用のセッションキーKs2bを生成する（ステップS625）。そして、ライセンス管理モジュール511は、生成したセッションキーKs2bをメモリカード110から受信したクラス公開暗号鍵KPm3によって暗号化し、暗号化データ{Ks2b}Km3を生成し（ステップS626）、暗号化データ{Ks2b}Km3にダミートランザクションIDを追加したダミートランザクションID//{Ks2b}Km3をUSBインタフェース550、端子580、およびUSBケーブル70を介して再生端末100へ送信する（ステップS627）。再生端末100のコントローラ106は、端子1114、USBインタフェース1112、およびBS3を介してダミートランザクションID//{Ks2b}Km3を受信し、その受信したダミートランザクションID//{Ks2b}Km3をメモリカードインタフェース1200を介してメモリカード110へ送信する。そして、メモリカード110のコントローラ1420は、端子1426、インタフェース1424およびバスBS4を介してダミートランザクションID//{Ks2b}Km3を受信する（ステップS628）。復号処理部1422は、コントローラ1420からバスBS4を介して{Ks2b}Km3を受取り、Km保持部1421からのクラス秘密復号鍵Km3によって{Ks2b}Km3を復号してセッションキーKs2bを受理する（ステップS629）。そして、セッションキー発生部1418は、セッションキーKs2cを生成し（ステップS630）、コントローラ1420は、バスBS4を介してメモリ1415のCRL領域1415Aから禁止クラスリストの更新日時CRLdateを取得し、その取得した更新日時CRLdateを切換スイッチ1446へ与える（ステップS631）。

【0378】そうすると、暗号化処理部1406は、切換スイッチ1446の端子を順次切換えることによって取得したセッションキーKs2c、個別公開暗号鍵KPmc4および更新日時CRLdateを、復号処理部1422によって復号され、切換スイッチ1442の端子Paを介して取得したセッションキーKs2bによって暗号化し、暗号化データ{Ks2c//KPmc4//CRLdate}Ks2bを生成する。コントローラ1420は、暗号化データ{Ks2c//KPmc4//CRLdate}Ks2bをバスBS4、インタフェース1424および端子1426を介して再生端末100へ出力し、再生端末100のコントローラ1106は、メモリカードインタフェース1200を介して暗号化データ{Ks2c//KPmc4//CRLdate}Ks2bを受取る。そして、コントローラ1106は、暗号化データ{Ks2c//KPmc4//CRLdate}Ks2bをUSBインタフェース1112、端子1114、およびUSBケーブル70を介してパーソナルコンピュータ50へ送信する（ステップS632）。

【0379】パーソナルコンピュータ50のライセンス管理モジュール511は、端子580およびUSBインタフェース550を介して暗号化データ{Ks2c//KPmc4//CRLdate}Ks2bを受信し（ステップS633）、その受信した暗号化データ{Ks2c//KPmc4//CRLdate}Ks2bをセッションキーKs2bによって復号し、セッションキーKs2c、個別公開暗号鍵KPmc4および更新日時CRLdateを受理する（ステップS634）。

【0380】そうすると、ライセンス管理モジュール511は、受理した個別公開暗号鍵KPmc4がステップS617で取得した機密情報nのチェックアウト情報に含まれる否かを、すなわち、チェックアウトしようとするライセンスのチェックアウト用トランザクションIDに対応して格納されている個別公開暗号鍵KPmcxと一致するか否かを確認する（ステップS635）。

【0381】受理された個別公開暗号鍵KPmc4は、暗号化コンテンツデータおよびライセンスのチェックアウトの際に、更新されたチェックアウト情報に含まれるものである（図34のステップS551を参照）。したがって、暗号化コンテンツデータ等のチェックアウト先に対応する個別公開暗号鍵KPmc4をチェックアウト情報に含ませることによってチェックインの際にチェックアウトしたチェックアウト先を容易に特定することが

できる。

【0382】ステップS635において、個別公開暗号鍵KPmc4がチェックアウト情報に含まれていないときチェックイン動作は終了する（ステップS653）。ステップS635において、個別公開暗号鍵KPmc4がチェックアウト情報に含まれていると、ライセンス管理モジュール511は、ダミーライセンス、つまり、ダミートランザクションID、対応するコンテンツ存在しないダミーコンテンツID、再生に関与し得ないダミーライセンス鍵Kc（ダミーKcと表す。）、移動複製フラグが「移動複製禁止」かつ再生回数が「0」を示すダミーアクセス制限情報ACm（ダミーACmと表す。）、およびダミー再生期限ACp（ダミーACpと表す。）を個別公開暗号鍵KPmc4によって暗号化し、暗号化データ｛ダミートランザクションID//ダミーコンテンツID//Kc//ダミーACm//ダミーACp｝Kmc4を生成する（ステップS636）。

【0383】ライセンス管理モジュール511は、暗号化データ｛ダミートランザクションID//ダミーコンテンツID//ダミーKc//ダミーACm//ダミーACp｝Kmc4をセッションキーKs2cによって暗号化を行い、暗号化データ｛｛ダミートランザクションID//ダミーコンテンツID//ダミーKc//ダミーACm//ダミーACp｝Kmc4｝Ks2cを生成し、その生成した暗号化データ｛｛ダミートランザクションID//ダミーコンテンツID//Kc//ダミーACm//ダミーACp｝Kmc4｝Ks2cをUSBインタフェース550、端子580、およびUSBケーブル70を介して再生端末100へ送信する（ステップS637）。

【0384】再生端末100のコントローラ1106は、端子1114、USBインタフェース1112、およびバスBS3を介して暗号化データ｛｛ダミートランザクションID//ダミーコンテンツID//ダミーKc//ダミーACm//ダミーACp｝Kmc4｝Ks2cを受信する。コントローラ1106は、受信した暗号化データ｛｛ダミートランザクションID//ダミーコンテンツID//ダミーKc//ダミーACm//ダミーACp｝Kmc4｝Ks2cをバスBS3およびメモリカードインタフェース1200を介してメモリカード110へ送信する。そして、メモリカード110のコントローラ1420は、端子1426、端子1424、およびバスBS4を介して｛｛ダミートランザクションID//ダミーコンテンツID//ダミーKc//ダミーACm//ダミーACp｝Kmc4｝Ks2cを受信する（ステップS638）。

【0385】図38を参照して、メモリカード110の復号処理部1412は、｛｛ダミートランザクションID//ダミーコンテンツID//ダミーKc//ダミーACm//ダミーACp｝Kmc4｝Ks2cをバスBS4を介して受取り、セッションキー発生部1418によって発生されたセッションキーKs2cによって復号し、｛ダミートランザクションID//ダミーコンテンツID//ダミーKc//ダミーACm//ダミーACp｝Kmc4を受理する（ステップS639）。そして、復号処理部1404は、暗号化データ｛ダミートランザクションID//ダミーコンテンツID//ダミーKc//ダミーACm//ダミーACp｝Kmc4を復号処理部1412から受取り、その受取った暗号化データ｛ダミートランザクションID//ダミーコンテンツID//ダミーKc//ダミーACm//ダミーACp｝Kmc4をKmc保持部1402からの個別秘密復号鍵Kmc4によって復号し、ダミートランザクションID、ダミーコンテンツID、ダミーKc、ダミーACm、およびダミーACpを受理する（ステップS640）。

【0386】パーソナルコンピュータ50のライセンス管理モジュール511は、メモリカード110のライセンス管理ファイルに記載されているチェックアウトするライセンスが格納されているエントリ番号を取得して、ダミーライセンスを格納するためのエントリ番号として、USBインタフェース550、端子580、およびUSBケーブル70を介して再生端末102へ送信する（ステップS641）。そうすると、再生端末102のコントローラ1106は、端子1114、USBインタフェース1112、およびバスBS3を介してエントリ番号を受取り、バスBS4を介してその受取ったエントリ番号によって指定されるメモリ1415のライセンス領域1415Bに、ダミーライセンス（ダミートランザクションID、ダミーコンテンツID、ダミーライセンス鍵Kc、ダミーアクセス制限情報ACm、およびダミー再生期限ACp）を記録する（ステップS642）。このようにダミートランザクションID、ダミーコンテンツID、ダミーライセンス鍵Kc、ダミーアクセス制限情報ACm、およびダミー再生期限ACpを記録することによってメモリカード110へチェックアウトされたライセンスを消去することができる。

【0387】その後、パーソナルコンピュータ50のライセンス管理モジュール511は、チェックアウト情報内のチェックアウト可能数を1だけ増やし、チェックアウト用トランザクションID、およびチェックアウト先のメモリカードの個別公開鍵KPmc4を削除してチェックアウト情報を更新する（ステップS643）。そして、ライセンス管理モジュール511は、トランザクションID、コンテンツID、ライセンス鍵Kc、アクセス制限情報ACm、および再生期限ACpと更新したチェックアウト情報とを新たな機密情報nとして平文の機密ファイルを更新する（ステップS644）。その後、ライセンス管理モジュール511は、平文の機密ファイルをバインディング鍵Kbによって暗号化してHDD5

３０に記録されている暗号化機密ファイル１６０を更新する（ステップS６４５）。

【０３８８】そうすると、ライセンス管理モジュール５１１は、メモリカード１００のデータ領域１４１５Cに記録されているチェックインしたライセンスに対応するコンテンツファイル（暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆ）とライセンス管理ファイルを削除する削除指示をＵＳＢインタフェース５５０、端子５８０、およびＵＳＢケーブル７０を介して再生端末１００へ送信する（ステップS６４６）。再生端末１００のコントローラ１１０６は、端子１１１４、ＵＳＢインタフェース１１１２、およびバスＢＳ３を介してコンテンツファイル（暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆ）とライセンス管理ファイルの削除指示を受信する（ステップS６４７）。そうすると、コントローラ１１０６は、（暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆ）とライセンス管理ファイルとを削除する指示をメモリカード１１０へ出力し、メモリカード１１０のコントローラ１４２０は、端子１４２６、インタフェース１４２４、およびバスＢＳ４を介して暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆとライセンス管理ファイルとを削除するする指示を受信し、バスＢＳ４を介してメモリ１４１５の暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆ）とライセンス管理ファイルとを削除する（ステップS６４８）。

【０３８９】パーソナルコンピュータ５０のライセンス管理モジュール５１１は、チェックインした楽曲を削除した再生リストを作成し（ステップS６４９）、再生リストと、再生リストの書換指示とをメモリカード１１０へ送信する（ステップS６５０）。メモリカード１１０のコントローラ１４２０は、再生端末１００を介して再生リストと書換指示とを受信し（ステップS６５１）、バスＢＳ４を介してメモリ１４１５の再生リストを受信した再生リストに書換え（ステップS６５２）、チェックイン動作が終了する（ステップS６５３）。

【０３９０】このように、暗号化コンテンツデータおよびライセンスをチェックアウトした相手先から暗号化コンテンツデータおよびライセンスを返却して貰うことによって、ライセンスの移動が禁止されてるセキュリティレベルの低いライセンス管理モジュールからおよびライセンスが、セキュリティレベルの高いメモリカードへ貸出され、メモリカードにおいてセキュリティレベルの低いライセンス管理モジュールで取得したライセンスを送信できるため、再生端末においてセキュリティレベルの低いライセンス管理モジュールで取得したライセンスによって再生できる暗号化コンテンツデータを再生して楽しむことができる。

【０３９１】また、メモリカードへ貸出されたライセンスは、アクセス制限情報ＡＣｍによってメモリカードから他の記録機器（メモリカード、ライセンス管理デバイスおよびライセンス管理モジュール）に対して、チェックアウトしたライセンスが出力できないよう指定されているため、貸出したライセンスの流出することはない。貸出したライセンス管理モジュールに対してチェックイン〈返却〉することで、貸出したライセンスの権利が、貸出したライセンス管理モジュールに戻るようになっている。従って、著作者の意に反して複製ができることを許すものではなく、セキュリティレベルが低下する処理ではなく、著作権も保護されている。

【０３９２】［再生］次に、図３９および図４０を参照してメモリカード１１０に移動、およびチェックアウトされたコンテンツデータの再生端末１００（コンテンツ再生デバイスとも言う、以下同じ）における再生動作について説明する。なお、図２９における処理以前に、再生端末１０２のユーザは、再生リストファイルに従って、再生するコンテンツ（楽曲）を決定し、コンテンツファイルを特定し、ライセンス管理ファイルを取得していることを前提として説明する。

【０３９３】図３９を参照して、再生動作の開始とともに、再生端末１００のユーザから操作パネル１１０８を介して再生指示が再生端末１００にインプットされる（ステップS１０００）。そうすると、コントローラ１１０６は、バスＢＳ３を介して認証データ保持部１５００から認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａ２を読出し、メモリカードインタフェース１２００を介してメモリカード１１０へ認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａ２を出力する（ステップS１００２）。

【０３９４】そうすると、メモリカード１１０は、認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａ２を受理する（ステップS１００４）。そして、メモリカード１１０の復号処理部１４０８は、受理した認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａ２を、ＫＰａ保持部１４１４に保持されたレベル２認証鍵ＫＰａ２によって復号し（ステップS１００６）、コントローラ１４２０は復号処理部１４０８における復号処理結果から、認証処理を行なう。すなわち、認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａ２が正規の認証データであるか否かを判断する認証処理を行なう（ステップS１００８）。復号できなかった場合、ステップS１０４８へ移行し、再生動作は終了する。認証データが復号できた場合、コントローラ１４２０は、取得したクラス証明書Ｃｐ１がメモリ１４１５のＣＲＬ領域１４１５Ａから読出した禁止クラスリストＣＲＬに含まれるか否かを判断する（ステップS１０１０）。この場合、クラス証明書Ｃｐ１には識別番号が付与されており、コントローラ１４２０は、受理したクラス証明書Ｃｐ１の識別番号が禁止クラスリストＣＲＬの中に存在するか否かを判別する。クラス証明書Ｃｐ１が禁止クラスリストデータに含まれると判断されると、ステップS１０４８へ移行し、再生動作は終了する。

【０３９５】ステップＳ１０１０において、クラス証明書Ｃｐ１が禁止クラスリストデータＣＲＬに含まれていないと判断されると、メモリカード１１０のセッションキー発生部１４１８は、再生セッション用のセッションキーＫｓ２を発生させる（ステップＳ１０１２）。そして、暗号処理部１４１０は、セッションキー発生部１４１８からのセッションキーＫｓ２を、復号処理部１４０８で復号されたクラス公開暗号鍵ＫＰｐ１によって暗号化した｛Ｋｓ２｝Ｋｐ１をバスＢＳ３へ出力する（ステップＳ１０１４）。そうすると、コントローラ１４２０は、インタフェース１４２４および端子１４２６を介してメモリカードインタフェース１２００へ｛Ｋｓ２｝Ｋｐ１を出力する（ステップＳ１０１６）。再生端末１００のコントローラ１１０６は、メモリカードインタフェース１２００を介して｛Ｋｓ２｝Ｋｐ１を取得する。そして、Ｋｐ１保持部１５０２は、秘密復号鍵Ｋｐ１を復号処理部１５０４へ出力する。

【０３９６】復号処理部１５０４は、Ｋｐ１保持部１５０２から出力された、公開暗号鍵ＫＰｐ１と対になっている秘密復号鍵Ｋｐ１によって｛Ｋｓ２｝Ｋｐ１を復号し、セッションキーＫｓ２を暗号処理部１５０６へ出力する（ステップＳ１０１８）。そうすると、セッションキー発生部１５０８は、再生セッション用のセッションキーＫｓ３を発生させ、セッションキーＫｓ３を暗号処理部１５０６へ出力する（ステップＳ１０２０）。暗号処理部１５０６は、セッションキー発生部１５０８からのセッションキーＫｓ３を復号処理部１５０４からのセッションキーＫｓ２によって暗号化して｛Ｋｓ３｝Ｋｓ２を出力し、コントローラ１１０６は、バスＢＳ３およびメモリカードインタフェース１２００を介して｛Ｋｓ３｝Ｋｓ２をメモリカード１１０へ出力する（ステップＳ１０２２）。

【０３９７】そうすると、メモリカード１１０の復号処理部１４１２は、端子１４２６、インタフェース１４２４、およびバスＢＳ４を介して｛Ｋｓ３｝Ｋｓ２を入力する（ステップＳ１０２４）。

【０３９８】図４０を参照して、復号処理部１４１２は、セッションキー発生部１４１８によって発生されたセッションキーＫｓ２によって｛Ｋｓ３｝Ｋｓ２を復号して、再生端末１００で発生されたセッションキーＫｓ３を受理する（ステップＳ１０２６）。

【０３９９】再生端末のコントローラ１１０６は、メモリカード１１０から事前に取得した再生リクエスト曲のライセンス管理ファイルからライセンスの格納されているエントリ番号を取得し、メモリカードインタフェース１２００を介してメモリカード１１０へ取得したエントリ番号を出力する（ステップＳ１０２７）。

【０４００】エントリ番号の入力に応じて、コントローラ１４２０は、アクセス制限情報ＡＣｍを確認する（ステップＳ１０２８）。ステップＳ１０２８においては、メモリのアクセスに対する制限に関する情報であるアクセス制限情報ＡＣｍを、具体的には、再生回数を確認することにより、確認することにより、既に再生不可の状態である場合には再生動作を終了し、アクセス制限情報の再生回数に回数制限がある場合にはアクセス制限情報ＡＣｍの再生回数を更新（１減ずる）した後に次のステップに進む（ステップＳ１０３０）。一方、アクセス制限情報ＡＣｍの再生回数によって再生回数が制限されていない場合においては、ステップＳ１０３０はスキップされ、アクセス制限情報ＡＣｍは更新されることなく処理が次のステップ（ステップＳ１０３２）に進行される。

【０４０１】ステップＳ１０２８において、当該再生動作において再生が可能であると判断された場合には、メモリ１４１５のライセンス領域１４１５Ｂに記録された再生リクエスト曲のライセンス鍵Ｋｃおよび再生期限ＡＣｐがバスＢＳ４上に出力される（ステップＳ１０３２）。

【０４０２】得られたライセンス鍵Ｋｃと再生期限ＡＣｐは、切換スイッチ１４４６の接点Ｐｆを介して暗号化処理部１４０６に送られる。暗号化処理部１４０６は、切換スイッチ１４４２の接点Ｐｂを介して復号処理部１４１２より受けたセッションキーＫｓ３によって切換スイッチ１４４６を介して受けたライセンス鍵Ｋｃと再生期限ＡＣｐとを暗号化し、｛Ｋｃ／／ＡＣｐ｝Ｋｓ３をバスＢＳ４に出力する（ステップＳ１０３４）。

【０４０３】バスＢＳ４に出力された暗号化データは、インタフェース１４２４、端子１４２６、およびメモリカードインタフェース１２００を介して再生端末１００に送出される。

【０４０４】再生端末１００においては、メモリカードインタフェース１２００を介してバスＢＳ３に伝達される暗号化データ｛Ｋｃ／／ＡＣｐ｝Ｋｓ３を復号処理部１５１０によって復号処理を行ない、ライセンス鍵Ｋｃおよび再生期限ＡＣｐを受理する（ステップＳ１０３６）。復号処理部１５１０は、ライセンス鍵Ｋｃを復号処理部１５１６に伝達し、再生期限ＡＣｐをバスＢＳ３に出力する。

【０４０５】コントローラ１１０６は、バスＢＳ３を介して、再生期限ＡＣｐを受理して再生の可否の確認を行なう（ステップＳ１０４０）。

【０４０６】ステップＳ１０４０においては、再生期限ＡＣｐによって再生不可と判断される場合には、再生動作は終了される。

【０４０７】ステップＳ１０４０において再生可能と判断された場合、コントローラ１１０６は、メモリカードインタフェース１２００を介してメモリカード１１０のデータ領域１４１５Ｃにコンテンツファイルとして記録された暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを要求する。そうすると、メモリカード１１０のコントローラ１

４２０は、メモリ１４１５から暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを取得し、バスＢＳ４、インタフェース１４２４、および端子１４２６を介してメモリカードインタフェース１２００へ出力する（ステップＳ１０４２）。

【０４０８】再生端末１００のコントローラ１１０６は、メモリカードインタフェース１２００を介して暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを取得し、バスＢＳ３を介して暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを復号処理部１５１６へ与える。

【０４０９】そして、復号処理部１５１６は、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを復号処理部１５１０から出力されたコンテンツ鍵Ｋｃによって復号してコンテンツデータＤａｔａを取得する（ステップＳ１０４４）。

【０４１０】そして、復号されたコンテンツデータＤｃは音楽再生部１５１８へ出力され、音楽再生部１５１８は、コンテンツデータを再生し、ＤＡ変換器１５１９はディジタル信号をアナログ信号に変換して端子１５３０へ出力する。そして、音楽データは端子１５３０から外部出力装置を介してヘッドホン１３０へ出力されて再生される（ステップＳ１０４６）。これによって再生動作が終了する。

【０４１１】上記においては、メモリカード１１０に記録された暗号化コンテンツデータを再生端末１００によって再生する場合について説明したが、パーソナルコンピュータ５０，８０に、図７に示すコンテンツ再生デバイス１５５０を内蔵することによってライセンス管理モジュール５１１およびライセンス管理デバイス５２０によって受信された暗号化コンテンツデータを再生することが可能である。なお、ライセンス管理モジュール５１１によって取得された暗号化コンテンツデータをコンテンツ再生デバイス１５５０により再生する場合、ライセンス管理モジュール５１１は、ライセンス管理デバイス５２０に格納されたバインディング鍵Ｋｂを取得し、ＨＤＤ５３０に記録された暗号化機密ファイル１６０をバインディング鍵Ｋｂによって復号し、平文の機密ファイルからライセンスを読出してコンテンツ再生デバイス１５５０へ与える。

【０４１２】また、パーソナルコンピュータ５０，８０に暗号化コンテンツデータを再生するソフトウエアに従って機能する再生部を内蔵することによって、ライセンス管理モジュール５１１が取得した暗号化コンテンツデータをソフトウエアにより再生することが可能である。この場合も、ライセンス管理モジュール５１１は、ライセンス管理デバイス５２０に格納されたバインディング鍵Ｋｂを取得し、ＨＤＤ５３０に記録された暗号化機密ファイル１６０をバインディング鍵Ｋｂによって復号し、平文の機密ファイルからライセンスを読出してコンテンツ再生デバイス１５５０へ与える。コンテンツ再生デバイス１５５０を用いたハード的に機密性を持つ再生（レベル２）に比べて、ソフトウエアによる再生は、ソフト的に機密性を持つ再生（レベル１）であるためセキュリティレベルが低い処理である。ゆえに、ライセンス管理デバイス５２０にて保持されるライセンスは、このソフトウェアによる再生では使用できない。

【０４１３】［移動２］図１に示すデータ配信システムにおいて、パーソナルコンピュータ５０のライセンス管理モジュール５１１が取得した暗号化コンテンツデータおよびライセンスをパーソナルコンピュータ８０へ移動する動作について説明する。なお、この移動を［移動２］という。

【０４１４】図４１～図４８は、ライセンス管理モジュール５１１が取得した暗号化コンテンツデータおよびライセンスのパーソナルコンピュータ８０への移動を説明するための第１～第８のフローチャートである。なお、図４１における処理以前に、パーソナルコンピュータ５０のユーザは、コンテンツリストファイルに従って、移動するコンテンツを決定し、ＨＤＤ５３０およびメモカード１１０のコンテンツファイルおよびライセンス管理ファイルが特定していることを前提に説明する。また、受信側のパーソナルコンピュータ８０におけるライセンス管理モジュールのクラスを識別する自然数ｗはｗ＝５であり、ライセンス管理モジュールを識別する自然数ｙはｙ＝５とする。

【０４１５】図４１を参照して、パーソナルコンピュータ５０のキーボード５６０を介してパーソナルコンピュータ５０のライセンス管理モジュール５１１によって取得されたライセンスの移動リクエストが入力されると（ステップＳ８００）、パーソナルコンピュータ５０のライセンス管理モジュール５１１は、バインディング鍵取得処理を行う。図４１のステップＳ８０１から図４２のステップ８１５の一連の処理がバインディング鍵取得処理であり、配信２のフローチャートにおける図２０のステップＳ２７０から図２１のステップＳ２８４の一連の処理と同じである。ゆえに、説明を省略する。

【０４１６】バインディングライセンスを取得すると、パーソナルコンピュータ５０のライセンス管理モジュール５１１は、バスＢＳ２を介してＨＤＤ５３０から暗号化機密ファイル１６０を取得し、その取得した暗号化機密ファイル１６０をバインディング鍵Ｋｂによって復号して平文の機密ファイルを取得する（ステップＳ８１６）。その後、パーソナルコンピュータ５０のライセンス管理モジュール５１１は、ライセンス管理ファイルに記録された機密情報番号ｎに対応する機密ファイル内の機密情報ｎ（トランザクションＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、アクセス制限情報ＡＣｍ、再生期限ＡＣｐ、およびチェックアウト情報）を取得する（ステップＳ８１７）。

【０４１７】そうすると、パーソナルコンピュータ５０のライセンス管理モジュール５１１は、取得したアクセ

ス制限情報ＡＣｍに基づいて暗号化コンテンツデータの移動および複製が可能か否かを確認する（ステップＳ５１８）、つまり、ライセンス管理モジュール５１１は、取得したアクセス制限情報ＡＣｍの再生回数、移動複製フラグに基づいて、パーソナルコンピュータ８０へ移動しようとするライセンスがアクセス制限情報ＡＣｍによって暗号化コンテンツデータの移動および複製ができないライセンスになっていないか否かを確認する。

【０４１８】ステップＳ８１８において、暗号化コンテンツデータの移動および複製が禁止されていた場合、ステップＳ９０３へ移行し、移動動作は終了する。ステップＳ８１８において、暗号化コンテンツデータの移動および複製が禁止されていない場合、ステップＳ８１９へ移行する。そして、ライセンス管理モジュール５１１は、取得したチェックアウト情報に基づいてチェックアウトが可能か否かを確認する（ステップＳ８１９）。ステップＳ８１９において、チェックアウトが不可能であれば、チェックアウトが禁止されているので、ステップＳ９０３へ移行し、チェックアウト動作は終了する。ステップＳ８１９において、チェックアウト可能であれば、新たなバインディング鍵を、ライセンス管理デバイス５２０に格納できるかを確認するためにデバイス確認処理を行なうデバイス確認処理において、ライセンス管理デバイス５２０が認証できない、あるいは、禁止クラスリストＣＲＬにより、新たなバインディング鍵が記録できない場合には、現状を維持するために、処理は中断する。図４２のステップＳ８２１から図４３のステップ８３３の一連の処理がデバイス確認処理であり、初期化のフローチャートにおける図１０のステップＳ１６から図１１のステップＳ４２の一連の処理と同じである。ゆえに、説明を省略する。

【０４１９】デバイス確認処理が終了すると、パーソナルコンピュータ５０のライセンス管理モジュール５１１は、認証データの送信要求を通信ケーブル９０を介してパーソナルコンピュータ８０へ送信する（ステップＳ８３４）。そうすると、パーソナルコンピュータ８０のライセンス管理モジュールは、認証データの送信要求を受信する（ステップＳ８３５）。

【０４２０】パーソナルコンピュータ８０のライセンス管理モジュールは、認証データの送信要求を受信すると、認証データ｛ＫＰｍ５／／Ｃｍ５｝ＫＰａ１をパーソナルコンピュータ５０へ送信する（ステップＳ８３６）。パーソナルコンピュータ５０のライセンス管理モジュール５１１は、端子５８０およびＵＳＢインタフェース５５０を介して認証データ｛ＫＰｍ５／／Ｃｍ５｝ＫＰａ１を受信し（ステップＳ８３７）、その受信した認証データ｛ＫＰｍ５／／Ｃｍ５｝ＫＰａ１をレベル１認証鍵ＫＰａ１によって復号する（ステップＳ８３８）。

【０４２１】図４４を参照して、ライセンス管理モジュール５１１は、復号処理結果から、処理が正常に行なわれたか否か、すなわち、メモリカード１１０が正規のメモリカードからのクラス公開暗号鍵ＫＰｍ５とクラス証明書Ｃｍ５とを保持することを認証するために、正規の機関でその正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行なう（ステップＳ８３９）。正当な認証データであると判断された場合、ライセンス管理モジュール５１１は、公開暗号鍵ＫＰｍ３および証明書Ｃｍ３を承認し、受理する。そして、次の処理（ステップＳ８４０）へ移行する。正当な認証データでない場合には、非承認とし、クラス公開暗号鍵ＫＰｍ５およびクラス証明書Ｃｍ５を受理しないで処理を終了する（ステップＳ９０３）。認証の結果、正規のメモリカードであることが認識されると、ライセンス管理モジュール５１１は、次に、メモリカード１１０のクラス証明書Ｃｍ３が禁止クラスリストＣＲＬにリストアップされているかどうかをＨＤＤ５３０に照会し、これらのクラス証明書が禁止クラスリストの対象になっている場合には、ここで移動動作を終了する（ステップＳ９０３）。一方、メモリカード１１０のクラス証明書が禁止クラスリストの対象外である場合には次の処理に移行する（ステップＳ８４０）。

【０４２２】認証の結果、正当な認証データを持つメモリカードを備える再生端末からのアクセスであり、クラスが禁止クラスリストの対象外であることが確認されるとライセンス管理モジュール５１１は、移動用のセッションキーＫｓ２ｄを生成する（ステップＳ８４１）。そして、ライセンス管理モジュール５１１は、生成したセッションキーＫｓ２ｄをパーソナルコンピュータ８０から受信したクラス公開暗号鍵ＫＰｍ５によって暗号化し、暗号化データ｛Ｋｓ２ｄ｝Ｋｍ５を生成し（ステップＳ８４２）、暗号化データ｛Ｋｓ２ｄ｝Ｋｍ５にトランザクションＩＤを追加したトランザクションＩＤ／／｛Ｋｓ２ｄ｝Ｋｍ５を通信ケーブル９０を介してパーソナルコンピュータ８０へ送信する（ステップＳ８４３）。パーソナルコンピュータ８０のライセンス管理モジュールは、トランザクションＩＤ／／｛Ｋｓ２ｄ｝Ｋｍ５を受信する（ステップＳ８４４）。そして、パーソナルコンピュータ８０のライセンス管理モジュールは、クラス秘密復号鍵Ｋｍ３によって｛Ｋｓ２ｄ｝Ｋｍ５を復号してセッションキーＫｓ２ｄを受理する（ステップＳ８４５）。そして、パーソナルコンピュータ８０のライセンス管理モジュールは、セッションキーＫｓ２ｅを生成し（ステップＳ８４６）、ＨＤＤから禁止クラスリストＣＲＬの更新日時ＣＲＬｄａｔｅを取得する（ステップＳ８４７）。

【０４２３】そして、パーソナルコンピュータ８０のライセンス管理モジュールは、セッションキーＫｓ２ｅ、個別公開暗号鍵ＫＰｍｃ５および禁止クラスリストＣＲＬｄａｔｅをセッションキーＫｓ２ｄによって暗号化

し、暗号化データ{Ｋｓ２ｅ//ＫＰｍｃ５//ＣＲＬｄａｔｅ}Ｋｓ２ｄを生成し、暗号化データ{Ｋｓ２ｅ//ＫＰｍｃ５//ＣＲＬｄａｔｅ}Ｋｓ２ｄを通信ケーブル９０を介してパーソナルコンピュータ５０へ送信する（ステップＳ８４８）。

【０４２４】パーソナルコンピュータ５０のライセンス管理モジュール５１１は、端子５８０およびＵＳＢインタフェース５５０を介して暗号化データ{Ｋｓ２ｅ//ＫＰｍｃ５//ＣＲＬｄａｔｅ}Ｋｓ２ｄを受信し（ステップＳ８４９）、その受信した暗号化データ{Ｋｓ２ｅ//ＫＰｍｃ５//ＣＲＬｄａｔｅ}Ｋｓ２ｄをセッションキーＫｓ２ｄによって復号し、セッションキーＫｓ２ｅ、個別公開暗号鍵ＫＰｍｃ５および更新日時ＣＲＬｄａｔｅを受理する（ステップＳ８５０）。そして、ライセンス管理モジュール５１１は、トランザクションＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、アクセス制限情報ＡＣｍ、および再生期限ＡＣｐをパーソナルコンピュータ８０に固有の個別公開暗号鍵ＫＰｍｃ５によって暗号化して暗号化データ{トランザクションＩＤ//コンテンツＩＤ//Ｋｃ//ＡＣｍ//ＡＣｐ}Ｋｍｃ５を生成する（ステップＳ８５１）。

【０４２５】図４５を参照して、パーソナルコンピュータ５０のライセンス管理モジュール５１１は、パーソナルコンピュータ８０のライセンス管理モジュールから送信された禁止クラスリストの更新日時ＣＲＬｄａｔｅに基づいてパーソナルコンピュータ８０のライセンス管理モジュールが管理する禁止クラスリストと自身の管理する禁止クラスリストのどちらが新しいか判断し、自身の管理する禁止クラスリストＣＲＬが古いと判断されたとき、ステップＳ８５３へ移行する。また、逆に、自身の管理する禁止クラスリストＣＲＬの方が新しいと判断されたときはステップＳ８５６へ移行する（ステップＳ８５２）。

【０４２６】自身の管理する禁止クラスリストＣＲＬが古いと判断されたとき、ライセンス管理モジュール５１１は、暗号化データ{トランザクションＩＤ//コンテンツＩＤ//Ｋｃ//ＡＣｍ//ＡＣｐ}Ｋｍｃ５をライセンス管理モジュール５１１において発生されたセッションキーＫｓ２ｅによって暗号化を行い、暗号化データ{{トランザクションＩＤ//コンテンツＩＤ//Ｋｃ//ＡＣｍ//ＡＣｐ}Ｋｍｃ５}Ｋｓ２ｅを通信ケーブル９０を介してパーソナルコンピュータ８０へ送信する（ステップＳ８５３）。

【０４２７】そして、パーソナルコンピュータ８０のライセンス管理モジュールは、暗号化データ{{トランザクションＩＤ//コンテンツＩＤ//Ｋｃ//ＡＣｍ//ＡＣｐ}Ｋｍｃ５}Ｋｓ２ｅを受信し（ステップＳ８５４）、暗号化データ{{トランザクションＩＤ//コンテンツＩＤ//Ｋｃ//ＡＣｍ//ＡＣｐ}Ｋｍｃ５}Ｋｓ２ｅをセッションキーＫｓ２ｅによって復号し、{トランザクションＩＤ//コンテンツＩＤ//Ｋｃ//ＡＣｍ//ＡＣｐ}Ｋｍｃ５を受理する（ステップＳ８５５）。その後、ステップＳ８６１へ移行する。

【０４２８】一方、ステップＳ８５２において、自身の管理する禁止クラスリストＣＲＬが新しいと判断されると、パーソナルコンピュータ５０のライセンス管理モジュール５１１は、ＨＤＤ５３０から禁止クラスリストＣＲＬを取得する（ステップＳ８５６）。そして、ライセンス管理モジュール５１１は、禁止クラスリストＣＲＬと暗号化データ{トランザクションＩＤ//コンテンツＩＤ//Ｋｃ//ＡＣｍ//ＡＣｐ}Ｋｍｃ５とを受けて、セッションキーＫｓ２ｅによって暗号化して暗号化データ{ＣＲＬ//{トランザクションＩＤ//コンテンツＩＤ//Ｋｃ//ＡＣｍ//ＡＣｐ}Ｋｍｃ５}Ｋｓ２ｅを通信ケーブル９０を介してパーソナルコンピュータ８０に送信する（ステップＳ８５７）。

【０４２９】パーソナルコンピュータ８０は、送信された暗号化データ{ＣＲＬ//{トランザクションＩＤ//コンテンツＩＤ//Ｋｃ//ＡＣｍ//ＡＣｐ}Ｋｍｃ５}Ｋｓ２ｅを受信し（ステップＳ８５８）、ライセンス管理モジュールは、セッションキーＫｓ２ｅを用いて受信データを復号してＣＲＬと暗号化データ{トランザクションＩＤ//コンテンツＩＤ//Ｋｃ//ＡＣｍ//ＡＣｐ}Ｋｍｃ５と受理する（ステップＳ８５９）。

【０４３０】パーソナルコンピュータ８０のライセンス管理モジュールは、ＨＤＤに記録された禁止クラスリストＣＲＬを受理したＣＲＬによって書換える（ステップＳ８６０）。

【０４３１】ステップＳ８５３，Ｓ８５４，Ｓ８５５は、パーソナルコンピュータ８０から送られてきた禁止クラスリストの更新日時ＣＲＬｄａｔｅによってが、受信側のパーソナルコンピュータ８０の保持する禁止クラスリストＣＲＬが送賃側のパーソナルコンピュータ５０の保持する禁止クラススリストＣＲＬの方が新しい場合のライセンス鍵Ｋｃ等のパーソナルコンピュータ８０への移動動作であり、ステップＳ８５４，Ｓ８５５，Ｓ８５６，Ｓ８５７，Ｓ８６０は、受信側のパーソナルコンピュータ８０の保持する禁止クラスリストＣＲＬが送信側のパーソナルコンピュータ５０の保持する禁止クラススリストＣＲＬの方が古い場合のライセンス鍵Ｋｃ等のパーソナルコンピュータ８０への移動動作である。

【０４３２】ステップＳ８５５またはステップＳ８６０の後、パーソナルコンピュータ８０のライセンス管理モジュールは、暗号化データ{トランザクションＩＤ//コンテンツＩＤ//Ｋｃ//ＡＣｍ//ＡＣｐ}Ｋｍｃ５は、個別秘密復号鍵Ｋｍｃ５によって復号し、ライセンス（ライセンス鍵Ｋｃ、トランザクションＩＤ、コンテンツＩＤ、アクセス制限情報ＡＣｍおよび再生期限ＡＣｐ）を受理する（ステップＳ８６１）。そして、ライ

センス管理モジュールは、受理したアクセス制限情報ＡＣｍによって再生回数が制限されているか否かを判別し、再生回数が制限されていないときステップＳ８６３へ移行し、再生回数が制限されているときステップＳ８６４へ移行する（ステップＳ８６２）。そして、再生回数が制限されていなとき、ライセンス管理モジュールは、パーソナルコンピュータ５０から受信した暗号化コンテンツおよびライセンスを他の装置へ貸出すためのチェックアウト可能数を含むチェックアウト情報を生成する（ステップＳ８６３）。この場合、チェックアウトの初期値は「３」に設定される。また、再生回数が制限されているとき、ライセンス管理モジュールは、暗号化コンテンツデータを他の装置へ貸出すためのチェックアウト可能数を「０」に設定してチェックアウト情報を生成する（ステップＳ８６４）。その後、図４６のステップＳ８８０へ移行する。

【０４３３】ステップＳ８５３またはステップＳ８５７の後、パーソナルコンピュータ５０がライセンスをパーソナルコンピュータ８０へ移動するのと並行してパーソナルコンピュータ５０が保持するバインディングライセンスの書換え動作が行なわれる。ステップＳ８５３またはステップＳ８５７の後、パーソナルコンピュータ５０のライセンス管理モジュール５１１は、アクセス制限情報ＡＣｍに基づいてライセンスの複製が可能か否かを判別する（ステップ８６５）。そして、ライセンスの複製が可能な場合、図４８のステップＳ８９８へ以降し、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆをパーソナルコンピュータ８０へ送信する。ステップＳ８６５において、ライセンスのアクセス制限情報ＡＣｍの移動復号フラグによって移動のみ可の場合、ライセンス管理モジュール５１１は、ＨＤＤ５３０に記録された移動させたライセンスに関するコンテンツリストファイル１５０のライセンス管理ファイル１５２ｎを読出し、ライセンス管理ファイルに記録された機密情報番号ｎを、ライセンス無に変更してライセンス管理ファイル１５２ｎを更新し（ステップＳ８６６）、最初の生成したバインディング鍵Ｋｂと異なる新たにバインディング鍵Ｋｂｂを生成する（ステップＳ８６７）。そして、ライセンス管理モジュール５１１は、平文の機密ファイル内の機密情報ｎを削除し、機密ファイルを新たに生成したバインディング鍵Ｋｂｂによって暗号化してＨＤＤ５３０内の暗号化機密ファイル１６０を更新する（ステップＳ８６８）。

【０４３４】図４６を参照して、ライセンス管理モジュール５１１は、新たに生成したバインディング鍵Ｋｂｂをライセンス管理デバイス５２０に格納するためにステップＳ８６９からステップＳ８７９のバインディング鍵登録処理を行う。初期化のフローチャートにおける図１１のステップＳ４４から図１２のステップＳ６６の一連の処理と同じ処理であり、バインディング鍵Ｋｂが、新たなバインディング鍵Ｋｂｂにセッション鍵Ｋｓ２ｂがセッション鍵Ｋｓ２ｃに変更されているのみである。ゆえに、説明を省略する。

【０４３５】新たなバインディング鍵Ｋｂｂの登録が終了すると、図４８のステップＳ８９８へ移行する。

【０４３６】図４７を参照して、図４５のステップＳ８６１またはステップＳ８６２の後、パーソナルコンピュータ８０においては、内蔵するライセンス管理モジュールからのバインディング鍵Ｋｂ２の取得、すなわちバインディング鍵の取得処理を行う。パーソナルコンピュータ８０においても、パーソナルコンピュータ５０と同じであり、ステップＳ８７８から図４８ステップＳ８９３に至る一連の処理がバインディング鍵取得処理であり、配信２のフローチャートにおける図２０のステップＳ２７０から図２１のステップＳ２８４に至る一連の処理と同じであり、取得するバインディングライセンス（トランザクションＩＤｂ２、コンテンツＩＤｂ２、バインディング鍵Ｋｂ２、および制御情報ＡＣｍｂ２，ＡＣｐｂ２）に、また、セッション鍵Ｋｓ２ａとＫｓ２ｂは、それぞれＫｓ２ｇとＫｓ２ｆに変更されているのみである。ゆえに、説明を省略する。

【０４３７】バインディング鍵Ｋｂ２を取得すると、パーソナルコンピュータ８０のライセンス管理モジュールは、バスＢＳ２を介してＨＤＤ５３０から暗号化機密ファイル１６０を取得し、その取得した暗号化機密ファイル１６０をバインディング鍵Ｋｂ２によって復号して平文の機密ファイルを取得する（ステップＳ８９５）。その後、ライセンス管理モジュールは、パーソナルコンピュータ５０から受信したライセンス（トランザクションＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、アクセス制限情報ＡＣｍ、再生期限ＡＣｐ）およびチェックアウト情報を新たな機密情報ｎ２として平文の機密ファイルに追記する（ステップＳ８９６）。そして、ライセンス管理モジュールは、平文の機密ファイルをバインディング鍵Ｋｂ２によって暗号化してＨＤＤに記録されている暗号化機密ファイル１６０を更新する（ステップＳ８９７）。

【０４３８】そうすると、パーソナルコンピュータ５０のライセンス管理モジュール５１１は、図４５のステップＳ８６８およびステップＳ８９７が共に終了すると、ＨＤＤ５３０に記録されているコンテンツファイル（暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆ）を読出し、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆとを通信ケーブル９０を介してパーソナルコンピュータ８０へ送信する（ステップＳ８９８）。

【０４３９】パーソナルコンピュータ８０のライセンス管理モジュールは、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆとを受信し、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆとを受理

する（ステップS899）。そして、ライセンス管理モジュールは、受理した暗号化コンテンツデータ{Dc}Kcと付加情報Dc-inf とをバスBS2をコンテンツファイルとして介してHDDに記録する（ステップS900）。また、ライセンス管理モジュールは、機密情報番号n2、トランザクションIDおよびコンテンツIDを含む、暗号化コンテンツデータ{Dc}Kcと付加情報Dc-inf とを記録したコンテンツファイルに対するライセンス管理ファイルを作成してHDDに記録する（ステップS901）。そして、ライセンス管理モジュールは、HDDに記録されているコンテンツリストファイルのコンテンツファイルに受理したコンテンツの名称を追記し（ステップS902）、移動動作が終了する（ステップS903）。

【0440】このように、パーソナルコンピュータ50のライセンス管理モジュール511が取得した暗号化コンテンツデータのライセンスをバインディング鍵Kbによって管理することによって、パーソナルコンピュータ50からパーソナルコンピュータ80へ暗号化コンテンツデータおよびライセンスを移動することができる。

【0441】実施の形態1によれば、パーソナルコンピュータに内蔵されたライセンス管理モジュールがソフトウエアによって取得した暗号化コンテンツデータのライセンスをライセンス管理デバイスによりハード的に管理されるバインディング鍵によって管理するので、ライセンス管理デバイスによって取得された暗号化コンテンツデータのライセンスと同じように「移動」という概念によって他のパーソナルコンピュータへ暗号化コンテンツデータおよびライセンスを送信することが可能である。

【0442】［実施の形態2］図49を参照して、ライセンス管理モジュール511によって取得された暗号化コンテンツデータのライセンスの実施の形態2における管理方法について説明する。

【0443】コンテンツリストファイル150の構成は実施の形態1における構成と同じである。HDD530には、暗号化機密ファイル160が記録されており、これには、ライセンス管理デバイス520に格納されたトランザクションIDb、コンテンツIDb、およびバインディング鍵Kbと同じものが格納されている。そして、暗号化機密ファイル160は、パーソナルコンピュータ50のCPUのシリアル番号等に依存した、パーソナルコンピュータ50から持ち出し不可能となるように独自の暗号化が施されている。また、ライセンス管理ファイル1522，・・，152nの内、ライセンス管理モジュール511によって取得されたライセンスに対するライセンス管理ファイルでは、ライセンス管理ファイル1522および152nがそれに当たる。ライセンスおよびチェックアウト情報を含む機密情報を、暗号化機密ファイルと同様に暗号化した暗号化機密情報と、ライセンスに関する平文情報とを含んでいる。バインディングライセンスは格納するライセンス管理デバイス520のエントリ番号「0」に常に格納する。

【0444】また、ライセンス管理デバイスにライセンスを格納したライセンスに対するライセンス管理ファイル、ライセンス管理ファイル1521および152nがこれに当たる、暗号化機密情報に換えて、ライセンス管理デバイスのライセンス領域1415Bのライセンスするエントリを特定するエントリ番号化記録されている。他のファイルおよびライセンス領域1415Bの構成については、実施の形態1の図25と同じであるので説明を省略する。

【0445】ライセンス管理ファイル1522，・・，152nからライセンスを取出すときは、ライセンス管理ファイル1522，・・，152nが暗号化機密情報含んでいれば、ライセンス管理デバイス520にエントリ番号「0」を送信してライセンス管理デバイス520からバインディング鍵Kbを取得し、その取得したバインディング鍵Kbが暗号化機密ファイル160に格納されたバインディング鍵Kbに一致することを確認する。一致していれば、暗号化機密情報を復号して、ライセンスおよびチェックアウト情報を取得する。一致しなければライセンスの取得は禁止されるので処理を中止する。一方、エントリ番号が含まれる場合には、ライセンス管理デバイス520に処理を任せる。さらには、ライセンス無の場合には、ライセンスは存在しないので処理を中止する。したがって、この実施の形態2においては、セキュリティレベルが低い（レベル1）のライセンに対する全ての処理において、ライセンス管理デバイス520に格納されたバインディング鍵Kbと暗号化機密ファイル160に格納されたバインディング鍵Kbとが一致しなければライセンス管理ファイル1522，・・，152nから暗号化コンテンツデータのライセンスを取出すことができないように運用する。

【0446】その結果、この実施の形態2においても、ライセンス管理モジュール511によって取得された暗号化コンテンツデータのライセンスは、バインディング鍵Kbによって管理することができ、実施の形態1で説明したのと同じようにパーソナルコンピュータ50からパーソナルコンピュータ80への暗号化コンテンツデータおよびライセンスの移動が可能となる。

【0447】［初期化］図50～図52は、実施の形態2における暗号化機密ファイル160の初期化を説明するための第1～第3のフローチャートである。図50～図52に示すフローチャートは、図10～図12にフローチャートのステップS66をステップS66aに代えたものであり、それ以外は図10～図12のフローチャートと同じである。したがって、図52を参照して、ステップS64の後、ライセンス管理モジュール511は、トランザクションIDb、コンテンツIDbおよびバインディング鍵Kbを平文の機密ファイルに格納し、

平文の機密ファイルに独自の暗号化を施して暗号化機密ファイル１６０を作成し、その作成した暗号化機密ファイル１６０をＨＤＤ５３０に記録する（ステップＳ６６ａ）。そして、初期化の動作は終了する（ステップＳ６８）。

【０４４８】［配信２］図５３～図５６は、実施の形態２において、ライセンス管理モジュール５１１から配信サーバ１０から暗号化コンテンツデータおよびライセンスを受信するときの動作を説明するための第１～第４のフローチャートである。図５３～図５６に示すフローチャートは、図１７～図２１に示すフローチャートのステップＳ２６６，Ｓ２６８とステップＳ２８８との間のステップをステップＳ２８７ａ～Ｓ２８７ａに代えたものであり、その他は、図１７～図２１に示すフローチャートと同じである。図５６を参照して、ステップＳ２６６，Ｓ２６８において、チェックアウト情報が生成された後、ライセンス管理モジュール５１１は、受理したライセンス（トランザクションＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、アクセス制限情報ＡＣｍおよび再生期限ＡＣｐ）とチェックアウト情報とバインディング情報とに独自の暗号化を施して暗号化機密情報を生成する（ステップＳ２８６ａ）。そして、ライセンス管理モジュール５１１は、生成した暗号化機密情報、トランザクションＩＤ、およびコンテンツＩＤを含むライセンス管理ファイルを作成してＨＤＤ５３０に記録する（ステップＳ２８７ａ）。その後、ステップＳ２８８へ移行して上述した各ステップが実行されて暗号化コンテンツデータおよびライセンスの配信動作が終了する。

【０４４９】［リッピング］図５７および図５８は、実施の形態２において、ライセンス管理モジュール５１１が音楽ＣＤから暗号化コンテンツデータおよびライセンスを取得するリッピングの動作を説明するための第１および第２のフローチャートである。図５７および図５８に示すフローチャートは、図２２～図２４に示すフローチャートのステップＳ７０８とステップＳ７２５との間のステップをステップをステップＳ７２０ａ～ステップＳ７２４ａに代えたものであり、それ以外は、図２２～図２４に示すフローチャートと同じである。図５８を参照して、ステップＳ７０８の後、ライセンス管理モジュール５１１は、受理したライセンス（トランザクションＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、アクセス制限情報ＡＣｍおよび再生期限ＡＣｐ）とチェックアウト情報とバインディング情報とに独自の暗号化を施して暗号化機密情報を生成する（ステップＳ７２３ａ）。そして、ライセンス管理モジュール５１１は、生成した暗号化機密情報、トランザクションＩＤ、およびコンテンツＩＤを含むライセンス管理ファイルを作成してＨＤＤ５３０に記録する（ステップＳ７２４ａ）。その後、ステップＳ７２５へ移行して上述した各ステップが実行されて暗号化コンテンツデータおよびライセンスのリッピングの動作が終了する。

【０４５０】［チェックアウト］図５９～図６３は、実施の形態２において、ライセンス管理モジュール５１１が取得した暗号化コンテンツデータおよびライセンスを再生端末１００に装着されたメモリカード１１０へチェックアウトする動作を説明するための第１～第５のフローチャートである。図５９～図６３に示すフローチャートは、図３０～図３４に示すフローチャートのステップＳ５１６，Ｓ５１７をステップＳ５１６ａ，Ｓ５１６ｂ，Ｓ５１７ａに代え、ステップＳ５５２，Ｓ５５３をステップＳ５５２ａ，５５３ａに代えたものであり、それ以外は、図３０～図３４に示すフローチャートと同じである。図６０を参照して、ステップＳ５１５の後、ライセンス管理モジュール５１１は、ＨＤＤ５３０に記録されている暗号化機密ファイル１６０を取得し、復号して格納されているバインディング鍵Ｋｂを取得する（ステップＳ５１６ａ）。そして、ライセンス管理モジュール５１１は、ライセンス管理デバイス５２０から取得したバインディング鍵Ｋｂが暗号化機密ファイル１６０から取得したバインディング鍵Ｋｂに一致するか否かを判別し、２つのバインディング鍵Ｋｂが相互に一致しないとき、ステップＳ５６４へ移行してチェックアウトの動作は終了する。２つのバインディング鍵Ｋｂが相互に一致するときは、次のステップＳ５１７ａへ移行する（ステップＳ５１６ｂ）。

【０４５１】ライセンス管理デバイス５２０から取得したバインディング鍵Ｋｂが暗号化機密ファイル１６０から取得したバインディング鍵Ｋｂに一致したとき、ライセンライセンス管理ファイルから暗号化機密情報を取得して、復号したライセンス（ライセンス鍵Ｋｃ、トランザクションＩＤ、コンテンツＩＤ、アクセス制限情報ＡＣｍおよび再生回数ＡＣｐ）を得る（ステップ５１７ａ）。そして、次のステップＳ５１１８へ移行する図６３を参照して、ステップＳ５５１の後、ライセンス管理モジュール５１１は、更新したチェックアウト情報を反映させた機密情報に独自の暗号化を施して暗号化機密情報を生成し（ステップＳ５５２ａ）、暗号化機密情報を含むライセンス管理ファイルを更新する（ステップＳ５５３ａ）。その後、ステップＳ５５４へ移行して上述した各ステップが実行されて暗号化コンテンツデータおよびライセンスのチェックアウトの動作が終了する。

【０４５２】このように、ライセンス管理デバイス５２０に格納されたバインディング鍵が暗号化機密ファイル１６０に格納されたバインディング鍵に一致する場合だけ、ライセンス管理モジュールは、ライセンス管理ファイルから暗号化コンテンツデータのライセンスを取得する。したがって、実施の形態２においても、バインディング鍵によって暗号化コンテンツデータのライセンスを実質的に管理する。

【０４５３】［チェックイン］図６４～図６７は、実施

の形態２において、ライセンス管理モジュール５１１が再生端末１００に装着されたメモリカード１１０へチェックアウトした暗号化コンテンツデータおよびライセンスをチェックインする動作を説明するための第１～第４のフローチャートである。図６４～図６７に示すフローチャートは、図３５～図３８に示すフローチャートのステップＳ６１６，Ｓ６１７をステップＳ６１６ａ，６１６ｂ，６１７ａに代え、ステップＳ６４３，Ｓ６４４をステップＳ６４３ａ，６４４ａに代えたものであり、それ以外は、図３５～図３８に示すフローチャートと同じである。

【０４５４】図６５を参照して、ステップＳ６１５の後、ライセンス管理モジュール５１１は、ＨＤＤ５３０に記録されている暗号化機密ファイル１６０を取得し、復号して格納されているバインディング鍵Ｋｂを取得する（ステップＳ６１６ａ）。そして、ライセンス管理モジュール５１１は、ライセンス管理デバイス５２０から取得したバインディング鍵Ｋｂが暗号化機密ファイル１６０から取得したバインディング鍵Ｋｂに一致するか否かを判別し、２つのバインディング鍵Ｋｂが相互に一致しないとき、ステップＳ６５３へ移行してチェックインの動作は終了する。２つのバインディング鍵Ｋｂが相互に一致するときは、次のステップＳ６１８へ移行する（ステップＳ６１６ｂ）。

【０４５５】ライセンス管理デバイス５２０から取得したバインディング鍵Ｋｂが暗号化機密ファイル１６０から取得したバインディング鍵Ｋｂに一致したとき、ライセンス管理ファイルから暗号化機密情報を取得して、復号したライセンス（ライセンス鍵Ｋｃ、トランザクションＩＤ、コンテンツＩＤ、アクセス制限情報ＡＣｍおよび再生回数ＡＣｐ）を得る（ステップ６１７ａ）。そして、次のステップＳ５１１８へ移行する。

【０４５６】図６７を参照して、ステップＳ６４２の後、ライセンス管理モジュール５１１は、更新したチェックアウト情報を反映させた機密情報に独自の暗号化を施して暗号化機密情報を生成し（ステップＳ６４４ａ）、暗号化機密情報を含むライセンス管理ファイルを更新する（ステップＳ６４５ａ）。その後、ステップＳ６４６へ移行して上述した各ステップが実行されて暗号化コンテンツデータおよびライセンスのチェックインの動作が終了する，

【０４５７】［移動２］図６８～図７４は、実施の形態２において、ライセンス管理モジュール５１１が受信した暗号化コンテンツデータおよびライセンスをパーソナルコンピュータ５０からパーソナルコンピュータ８０へ移動する動作を説明するための第１～第７のフローチャートである。図６８～図７４に示すフローチャートは、図３９～図４６に示すフローチャートのステップＳ８００とステップＳ８０１との間にステップＳ８００ａ～ステップＳ８００ｃを挿入し、ステップＳ８１５とステップＳ８２０との間のステップをステップＳ８１６ａ，８１７ａに代え、ステップＳ８６７をステップＳ８６７ａとステップＳ８６７ｂに代え、ステップＳ８６２，Ｓ８６３とステップＳ８９７との間のステップをステップＳ８９５ａ～８９６ａに代えたものであり、それ以外は、図３９～図４６に示すフローチャートと同じである。

【０４５８】図６８を参照して、ライセンス管理モジュール５１１は、ステップＳ８００の後、ライセンス管理モジュール５１１は、ライセンス管理ファイルの暗号化機密情報を復号して機密情報（トランザクションＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、アクセス制限情報ＡＣｍ、再生期限ＡＣｐ、チェックアウト情報を取得する（ステップＳ８００ａ）。そして、ライセンス管理モジュール５１１は、ステップＳ８００ａにおいて取得したＡＣｍに基づいて暗号化コンテンツデータおよびライセンスの移動および複製が可能か否かを判別する。そして、ライセンス管理モジュール５１１は、暗号化コンテンツデータおよびライセンスの移動および複製が禁止されているとき、ステップＳ９０３へ移行して移動動作は終了し、移動および複製が禁止されていないときステップＳ８００ｃへ移行する（ステップＳ８００ｂ）。

【０４５９】ライセンス管理モジュール５１１は、暗号化コンテンツデータおよびライセンスの移動および複製が可能であるとき、チェックアウト情報に基づいてチェックアウト可能か否かを判別し、不可能なときステップＳ９０３へ移行して移動動作は終了し、チェックアウト可能なときステップＳ８０１へ移行する。

【０４６０】図６９を参照して、ステップＳ８１５の後、ライセンス管理モジュール５１１は、ＨＤＤ５３０に記録されている暗号化機密ファイル１６０を取得し、復号して格納されているバインディング鍵Ｋｂを取得する（ステップＳ８１６ａ）。そして、ライセンス管理モジュール５１１は、ライセンス管理デバイス５２０から取得したバインディング鍵Ｋｂが暗号化機密ファイル１６０から取得したバインディング鍵Ｋｂに一致するか否かを判別し、２つのバインディング鍵Ｋｂが相互に一致しないとき、ステップＳ９０３へ移行して移動の動作は終了する。２つのバインディング鍵Ｋｂが相互に一致するときは、次のステップＳ８２０へ移行する（ステップＳ８１７ａ）。

【０４６１】図７２を参照して、ステップＳ８６７の後、ライセンス管理モジュール５１１は、平分の機密ファイルに格納されているバインディング鍵Ｋｂをバインディング鍵Ｋｂｂに書換へ（ステップＳ８６８ａ）、独自の暗号化を施した暗号化機密ファイルを生成して、ＨＤＤ５３０の暗号化機密ファイルと書き換える（ステップＳ８６８ｂ）。次いで、図７３のステップＳ８６９へ移行する。

【０４６２】図７４を参照してステップＳ８６２，Ｓ８６３において、チェックアウト情報が生成された後、ラ

イセンス管理モジュール５１１は、受理したライセンス（トランザクションＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、アクセス制限情報ＡＣｍおよび再生期限ＡＣｐ）とチェックアウト情報とに独自の暗号化を施して暗号化機密情報を生成する（ステップＳ８９５ａ）。そして、ライセンス管理モジュール５１１は、生成した暗号化機密情報、トランザクションＩＤ、およびコンテンツＩＤを含むライセンス管理ファイルを作成してＨＤＤ５３０に記録する（ステップＳ８９６ａ）。その後、ステップＳ８９７へ移行して上述した各ステップが実行されて暗号化コンテンツデータおよびライセンスの配信動作が終了する。

【０４６３】その他の部分については、実施の形態１と同じである。実施の形態２によれば、パーソナルコンピュータに内蔵されたライセンス管理モジュールがソフトウエアによって取得した暗号化コンテンツデータのライセンスをライセンス管理デバイスによりハード的に管理されるバインディング鍵によって管理するので、ライセンス管理デバイスによって取得された暗号化コンテンツデータのライセンスと同じように「移動」という概念によって他のパーソナルコンピュータへ暗号化コンテンツデータおよびライセンスを送信することが可能である。

【０４６４】なお、実施に形態１および２において、ライセンス管理デバイス５２０には、バインディングライセンスと配信によるライセンスが格納できるとしたが、バインディングライセンス専用の管理デバイスであってもかまわない。

【０４６５】また、バインディングライセンスを指定するためにエントリ番号を指定したが専用のエントリを持ち、高いレベルのライセンスと区別して扱ってもかまわない。

【０４６６】今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【図面の簡単な説明】

【図１】　本発明の実施の形態１におけるデータ配信システムを概念的に説明する概略図である。

【図２】　図１に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図３】　図１に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図４】　図１に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

【図５】　図１に示すデータ配信システムにおける配信サーバの構成を示す概略ブロック図である。

【図６】　図１に示すデータ配信システムにおけるパーソナルコンピュータの構成を示す概略ブロック図である。

【図７】　図１に示すデータ配信システムにおける再生端末の構成を示す概略ブロック図である。

【図８】　図１に示すデータ配信システムにおけるメモリカードの構成を示す概略ブロック図である。

【図９】　図６に示すパーソナルコンピュータに内蔵されたライセンス管理デバイスの構成を示す概略ブロック図である。

【図１０】　図１に示すパーソナルコンピュータにおける機密ファイルの初期化を説明するための第１のフローチャートである。

【図１１】　図１に示すパーソナルコンピュータにおける機密ファイルの初期化を説明するための第２のフローチャートである。

【図１２】　図１に示すパーソナルコンピュータにおける機密ファイルの初期化を説明するための第３のフローチャートである。

【図１３】　図１に示すデータ配信システムにおけるセキュリティレベルの高い配信動作を説明するための第１のフローチャートである。

【図１４】　図１に示すデータ配信システムにおけるセキュリティレベルの高い配信動作を説明するための第２のフローチャートである。

【図１５】　図１に示すデータ配信システムにおけるセキュリティレベルの高い配信動作を説明するための第３のフローチャートである。

【図１６】　図１に示すデータ配信システムにおけるセキュリティレベルの高い配信動作を説明するための第４のフローチャートである。

【図１７】　図１に示すデータ配信システムにおけるセキュリティレベルの低い配信動作を説明するための第１のフローチャートである。

【図１８】　図１に示すデータ配信システムにおけるセキュリティレベルの低い配信動作を説明するための第２のフローチャートである。

【図１９】　図１に示すデータ配信システムにおけるセキュリティレベルの低い配信動作を説明するための第３のフローチャートである。

【図２０】　図１に示すデータ配信システムにおけるセキュリティレベルの低い配信動作を説明するための第４のフローチャートである。

【図２１】　図１に示すデータ配信システムにおけるセキュリティレベルの低い配信動作を説明するための第５のフローチャートである。

【図２２】　図１に示すデータ配信システムにおけるリッピングの動作を説明するための第１のフローチャートである。

【図２３】　図１に示すデータ配信システムにおけるリッピングの動作を説明するための第２のフローチャートである。

【図２４】　図１に示すデータ配信システムにおけるリッピングの動作を説明するための第３のフローチャートである。
【図２５】　パーソナルコンピュータのハードディスクにおけるコンテンツリストファイルの構成を示す図である。
【図２６】　図１に示すデータ配信システムにおける暗号化コンテンツデータのライセンスの移動動作を説明するための第１のフローチャートである。
【図２７】　図１に示すデータ配信システムにおける暗号化コンテンツデータのライセンスの移動動作を説明するための第２のフローチャートである。
【図２８】　図１に示すデータ配信システムにおける暗号化コンテンツデータのライセンスの移動動作を説明するための第３のフローチャートである。
【図２９】　図１に示すデータ配信システムにおける暗号化コンテンツデータのライセンスの移動動作を説明するための第４のフローチャートである。
【図３０】　図１に示すデータ配信システムにおける暗号化コンテンツデータのライセンスのチェックアウト動作を説明するための第１のフローチャートである。
【図３１】　図１に示すデータ配信システムにおける暗号化コンテンツデータのライセンスのチェックアウト動作を説明するための第２のフローチャートである。
【図３２】　図１に示すデータ配信システムにおける暗号化コンテンツデータのライセンスのチェックアウト動作を説明するための第３のフローチャートである。
【図３３】　図１に示すデータ配信システムにおける暗号化コンテンツデータのライセンスのチェックアウト動作を説明するための第４のフローチャートである。
【図３４】　図１に示すデータ配信システムにおける暗号化コンテンツデータのライセンスのチェックアウト動作を説明するための第５のフローチャートである。
【図３５】　図１に示すデータ配信システムにおける暗号化コンテンツデータのライセンスのチェックイン動作を説明するための第１のフローチャートである。
【図３６】　図１に示すデータ配信システムにおける暗号化コンテンツデータのライセンスのチェックイン動作を説明するための第２のフローチャートである。
【図３７】　図１に示すデータ配信システムにおける暗号化コンテンツデータのライセンスのチェックイン動作を説明するための第３のフローチャートである。
【図３８】　図１に示すデータ配信システムにおける暗号化コンテンツデータのライセンスのチェックイン動作を説明するための第４のフローチャートである。
【図３９】　再生端末における再生動作を説明するための第１のフローチャートである。
【図４０】　再生端末における再生動作を説明するための第２のフローチャートである。
【図４１】　図１に示すデータ配信システムにおける暗号化コンテンツデータおよびライセンスのパーソナルコンピュータ間での移動を説明するための第１のフローチャートである。
【図４２】　図１に示すデータ配信システムにおける暗号化コンテンツデータおよびライセンスのパーソナルコンピュータ間での移動を説明するための第２のフローチャートである。
【図４３】　図１に示すデータ配信システムにおける暗号化コンテンツデータおよびライセンスのパーソナルコンピュータ間での移動を説明するための第３のフローチャートである。
【図４４】　図１に示すデータ配信システムにおける暗号化コンテンツデータおよびライセンスのパーソナルコンピュータ間での移動を説明するための第４のフローチャートである。
【図４５】　図１に示すデータ配信システムにおける暗号化コンテンツデータおよびライセンスのパーソナルコンピュータ間での移動を説明するための第５のフローチャートである。
【図４６】　図１に示すデータ配信システムにおける暗号化コンテンツデータおよびライセンスのパーソナルコンピュータ間での移動を説明するための第６のフローチャートである。
【図４７】　図１に示すデータ配信システムにおける暗号化コンテンツデータおよびライセンスのパーソナルコンピュータ間での移動を説明するための第７のフローチャートである。
【図４８】　図１に示すデータ配信システムにおける暗号化コンテンツデータおよびライセンスのパーソナルコンピュータ間での移動を説明するための第８のフローチャートである。
【図４９】　パーソナルコンピュータのハードディスクにおけるコンテンツリストファイルの他の構成を示す図である。
【図５０】　図１に示すパーソナルコンピュータにおける機密ファイルの初期化の他の動作を説明するための第１のフローチャートである。
【図５１】　図１に示すパーソナルコンピュータにおける機密ファイルの初期化の他の動作を説明するための第２のフローチャートである。
【図５２】　図１に示すパーソナルコンピュータにおける機密ファイルの初期化の他の動作を説明するための第３のフローチャートである。
【図５３】　図１に示すデータ配信システムにおけるセキュリティレベルの低い他の配信動作を説明するための第１のフローチャートである。
【図５４】　図１に示すデータ配信システムにおけるセキュリティレベルの低い他の配信動作を説明するための第２のフローチャートである。
【図５５】　図１に示すデータ配信システムにおけるセ

キュリティレベルの低い他の配信動作を説明するための第３のフローチャートである。

【図５６】　図１に示すデータ配信システムにおけるセキュリティレベルの低い他の配信動作を説明するための第４のフローチャートである。

【図５７】　図１に示すデータ配信システムにおけるリッピングの他の動作を説明するための第１のフローチャートである。

【図５８】　図１に示すデータ配信システムにおけるリッピングの他の動作を説明するための第２のフローチャートである。

【図５９】　図１に示すデータ配信システムにおける暗号化コンテンツデータのライセンスのチェックアウトの他の動作を説明するための第１のフローチャートである。

【図６０】　図１に示すデータ配信システムにおける暗号化コンテンツデータのライセンスのチェックアウトの他の動作を説明するための第２のフローチャートである。

【図６１】　図１に示すデータ配信システムにおける暗号化コンテンツデータのライセンスのチェックアウトの他の動作を説明するための第３のフローチャートである。

【図６２】　図１に示すデータ配信システムにおける暗号化コンテンツデータのライセンスのチェックアウトの他の動作を説明するための第４のフローチャートである。

【図６３】　図１に示すデータ配信システムにおける暗号化コンテンツデータのライセンスのチェックアウトの他の動作を説明するための第５のフローチャートである。

【図６４】　図１に示すデータ配信システムにおける暗号化コンテンツデータのライセンスのチェックインの他の動作を説明するための第１のフローチャートである。

【図６５】　図１に示すデータ配信システムにおける暗号化コンテンツデータのライセンスのチェックインの他の動作を説明するための第２のフローチャートである。

【図６６】　図１に示すデータ配信システムにおける暗号化コンテンツデータのライセンスのチェックインの他の動作を説明するための第３のフローチャートである。

【図６７】　図１に示すデータ配信システムにおける暗号化コンテンツデータのライセンスのチェックインの他の動作を説明するための第４のフローチャートである。

【図６８】　図１に示すデータ配信システムにおける暗号化コンテンツデータおよびライセンスのパーソナルコンピュータ間での他の移動を説明するための第１のフローチャートである。

【図６９】　図１に示すデータ配信システムにおける暗号化コンテンツデータおよびライセンスのパーソナルコンピュータ間での他の移動動作を説明するための第２のフローチャートである。

【図７０】　図１に示すデータ配信システムにおける暗号化コンテンツデータおよびライセンスのパーソナルコンピュータ間での他の移動動作を説明するための第３のフローチャートである。

【図７１】　図１に示すデータ配信システムにおける暗号化コンテンツデータおよびライセンスのパーソナルコンピュータ間での他の移動動作を説明するための第４のフローチャートである。

【図７２】　図１に示すデータ配信システムにおける暗号化コンテンツデータおよびライセンスのパーソナルコンピュータ間での他の移動動作を説明するための第５のフローチャートである。

【図７３】　図１に示すデータ配信システムにおける暗号化コンテンツデータおよびライセンスのパーソナルコンピュータ間での他の移動動作を説明するための第６のフローチャートである。

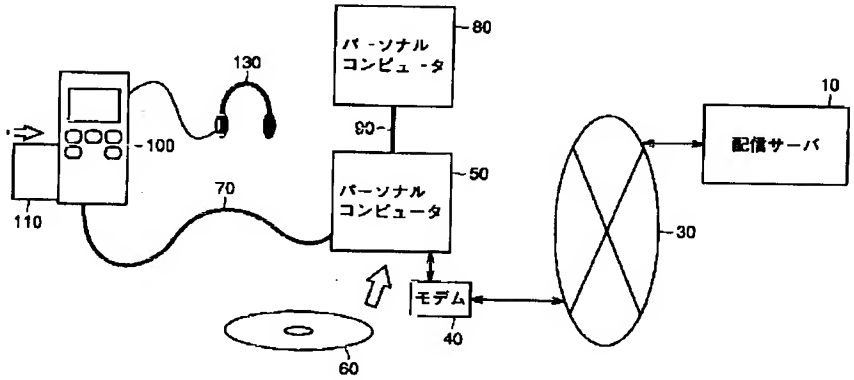
【図７４】　図１に示すデータ配信システムにおける暗号化コンテンツデータおよびライセンスのパーソナルコンピュータ間での他の移動動作を説明するための第７のフローチャートである。

【符号の説明】

１０　配信サーバ、２０　配信キャリア、３０　インターネット網、４０　モデム、５０，８０　パーソナルコンピュータ、６０　ＣＤ、７０　ＵＳＢケーブル、９０　通信ケーブル、１００　再生端末、１１０　メモリカード、１３０ヘッドホーン、１５０　コンテンツリストファイル、１６０　暗号化機密ファイル、３０２　課金データベース、３０４　情報データベース、３０６　ＣＲＬデータベース、３０７　メニューデータベース、３０８　配信記録データベース、３１０　データ処理部、３１２，３２０，１４０４，１４０８，１４１２，１４２２，１５０４，１５１０，１５１６，５２０４，５２０８，５２１２，５２２２　復号処理部、３１３　認証鍵保持部、３１５　配信制御部、３１６，　セッションキー発生部、３１８，３２６，３２８，１４０６，１４１０，１４１７，１５０６，５２０６，５２１０，５２１７，５４０５　暗号処理部、３５０　通信装置、５１０，１１０６，１４２０，５２２０　コントローラ、５１１　ライセンス管理モジュール、５２０　ライセンス管理デバイス、５３０　ハードディスク、５４０　ＣＤ－ＲＯＭドライブ、５５０，１１１２　ＵＳＢインタフェース、５６０　キーボード、５７０　ディスプレイ、５８０，１１１４，１４２６，１５３０，５２２６　端子、１１０８　操作パネル、１１１０　表示パネル、１２００　メモリカードインタフェース、１４００，１５００，５２００　認証データ保持部、１４０２，５２０２　Ｋｍｃ保持部、１４１４，５２１４　ＫＰａ保持部、１４１５，５２１５　メモリ、１４１５Ａ，５２１５Ａ　ＣＲＬ領域、１４１５Ｂ，５２１５Ｂ　ライセン

ス領域、１４１５Ｃ　データ領域、１４１６，５２１６　ＫＰｍｃ保持部、１４１８，５２１８　セッションキー発生部、１４２１，５２２１　Ｋｍ保持部、１４２４，５２２４　インタフェース、１４４２，１４４６　切換スイッチ、１５０２　Ｋｐ１保持部、１５１８　音楽再生部、１５１９　ＤＡ変換器、１５２１～１５２ｎ　ライセンス管理ファイル、１５３１～１５３ｎ　コンテンツファイル、１５５０　コンテンツ再生デバイス。

【図１】



【図２】

記号	種類	属性	特性
Dc	コンテンツデータ	コンテンツ固有	例：音楽データ、朗読データ、教材データ、画像データ Kcにて復号可能な暗号化コンテンツデータ {Dc}Kcとして配信され、メモリカードに保持される
Dc-inf	付加情報	コンテンツ固有	Dcに付随する平文データ。
Kc	ライセンス	コンテンツ固有	ライセンス鍵 暗号化コンテンツデータを復号する復号鍵
ACm/ACp	ライセンス	ライセンス固有	制限情報 再生やライセンスの取り扱いに対する制限事項
トランザクションID	ライセンス	ライセンス固有	配信を特定するための管理コード
コンテンツID	ライセンス	コンテンツ固有	コンテンツを特定するための管理コード
ライセンスID	ライセンス	ライセンス固有	トランザクションID＋コンテンツIDの総称
ライセンス	ライセンス	ライセンス固有	Kc＋ACm＋ACp＋ライセンスIDの総称
CRL	禁止クラスリスト	システム共通	使用禁止証明データのリスト CRLの更新日(CrlLdate)を含む

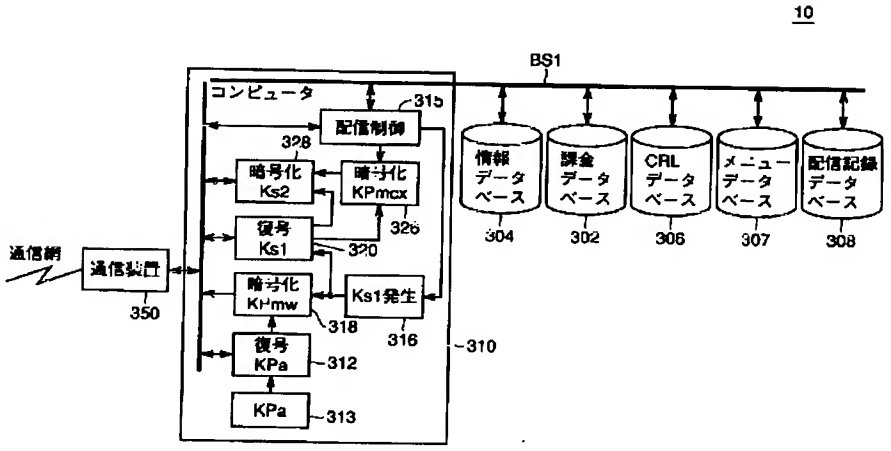
【図４】

記号	種類	特性
Kb	バインディングライセンス	バインディング鍵 ライセンスおよびチェックアウト管理情報を管理するための共通鍵
ACmb/ACpb		バインディングライセンスに対する制限情報 ACm：固定値(移動・複製禁止／再生回数制限なし) ACp：固定値(ダミー／無意味)
トランザクションIDb		バインディングライセンス用のトランザクションID （ライセンスにおけるトランザクションIDとは区別可）
コンテンツIDb		バインディングID用のダミーID
バインディングID		トランザクションIDb＋コンテンツIDbの総称
チェックアウト可能数	チェックアウト管理情報	チェックアウト可能なライセンス数 チェックアウトごとに1減算し、チェックインごとに1加算する。
チェックアウト先個別ID		チェックアウト先個別公開暗号鍵KPncx
チェックアウト時トランザクションID		チェックアウト時に用いられたトランザクションID

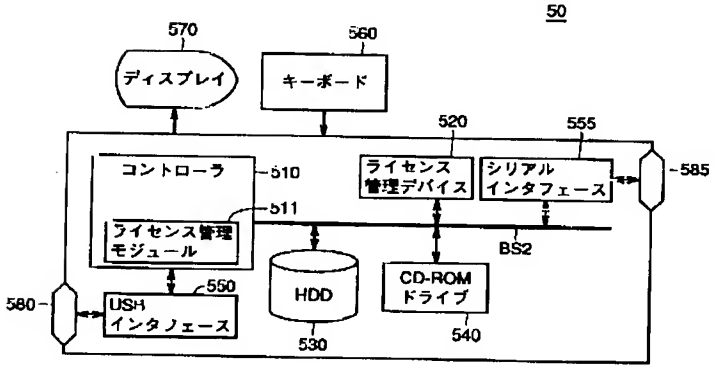
【図3】

	記号	機能	属性	特性
配信サーバ	KPa	公開認証鍵	システム共通	認証局にて認証された認証データを復号する鍵 セキュリティレベルに応じて2つの認証鍵KPa1(レベル1),KPa2(レベル2)がある。 メモリカードおよびコンテンツ管理モジュールと同一
	Ks1	共通鍵	セッション固有	メモリカード・ライセンス管理デバイス、ライセンス管理モジュールへのライセンス配信ごとに発生
メモリカード ライセンス管理デバイス(ハードタンパ)	KPa	公開認証鍵	システム共通	認証局にて認証された認証データを復号する鍵 配信サーバと同一
	KPmw	公開暗号鍵	クラス固有	証明書Cmwとともに認証局にて暗号化された認証データとして保持 wはクラスを識別するための識別子
	Kmw	秘密復号鍵	クラス固有	公開暗号鍵KPmwにて暗号化されたデータを復号する非対称な復号鍵
ライセンス管理モジュール(ソフトタンパ)	KPmcx	公開暗号鍵	個別	メモリカードごとに異なる。 xはモジュールを識別するための識別子
	Kmcx	秘密復号鍵	個別	公開暗号鍵KPmcxにて暗号化されたデータを復号する非対称な復号鍵
	Ks2	共通鍵	セッション固有	配信サーバまたは音楽再生モジュール間のライセンスの授受ごとに発生
	Cmw	証明書	クラス証明書	メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールのクラス証明書。認証機能を有する。 (KPmw//Cmw)KPaの形式で出荷時に記録。 ※メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールのクラスwごとに異なる。
コンテンツ再生デバイス	KPpy	公開暗号鍵	クラス固有	証明書Cmwとともに認証局にて暗号化された認証データとして保持 yはクラスを識別するための識別子
	Kpy	秘密復号鍵	クラス固有	公開暗号鍵KPpyにて暗号化されたデータを復号する非対称な復号鍵
	Ks3	共通鍵	セッション固有	配信サーバまたは音楽再生モジュール間の再生セッションごとに発生
	Cpy	証明書	クラス証明書	コンテンツ再生デバイスのクラス証明書。認証機能を有する。 (KPpy//Cpy)KPaの形式で出荷時に記録。 ※コンテンツ再生デバイスのクラスyごとに異なる。

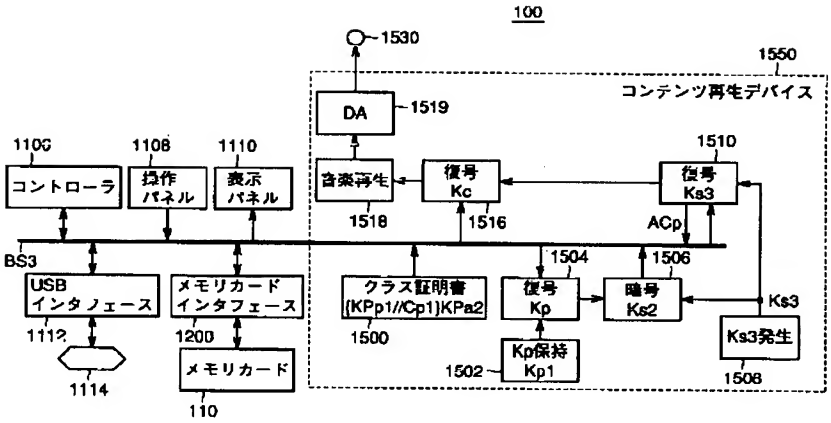
【図5】



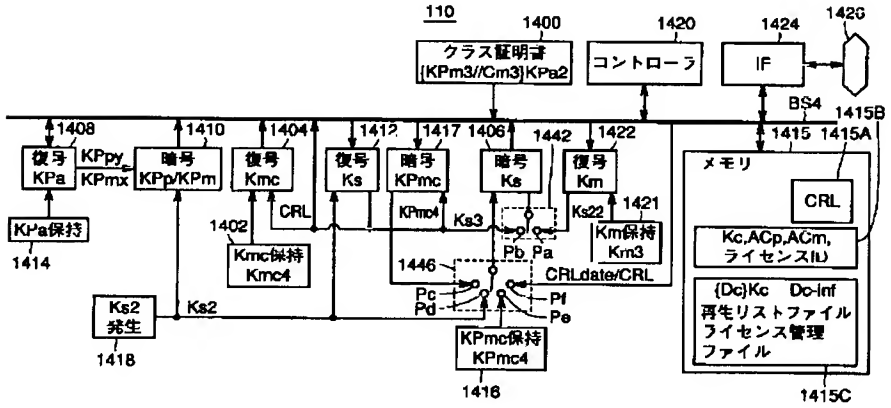
【図6】



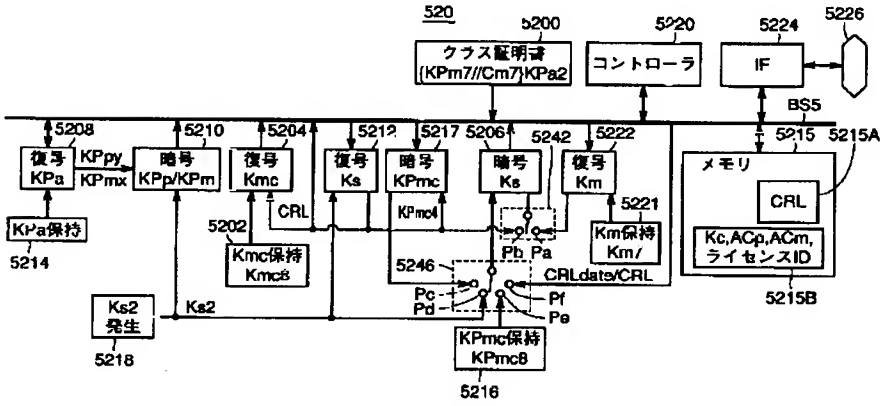
【図7】


100
1530
1550
コンテンツ再生デバイス
DA
1519
1100
1108
1110
コントローラ
操作パネル
表示パネル
音楽再生
1518
復号 Kc
1516
1510
復号 Ks3
ACp
BS3
1504
1506
USB インタフェース
メモリカード インタフェース
クラス証明書 {KPp1//Cp1}KPa2
1500
復号 Kp
暗号 Ks2
Ks3
Ks3発生
1508
1112
1200
Kp保持 Kp1
1502
1114
メモリカード
110

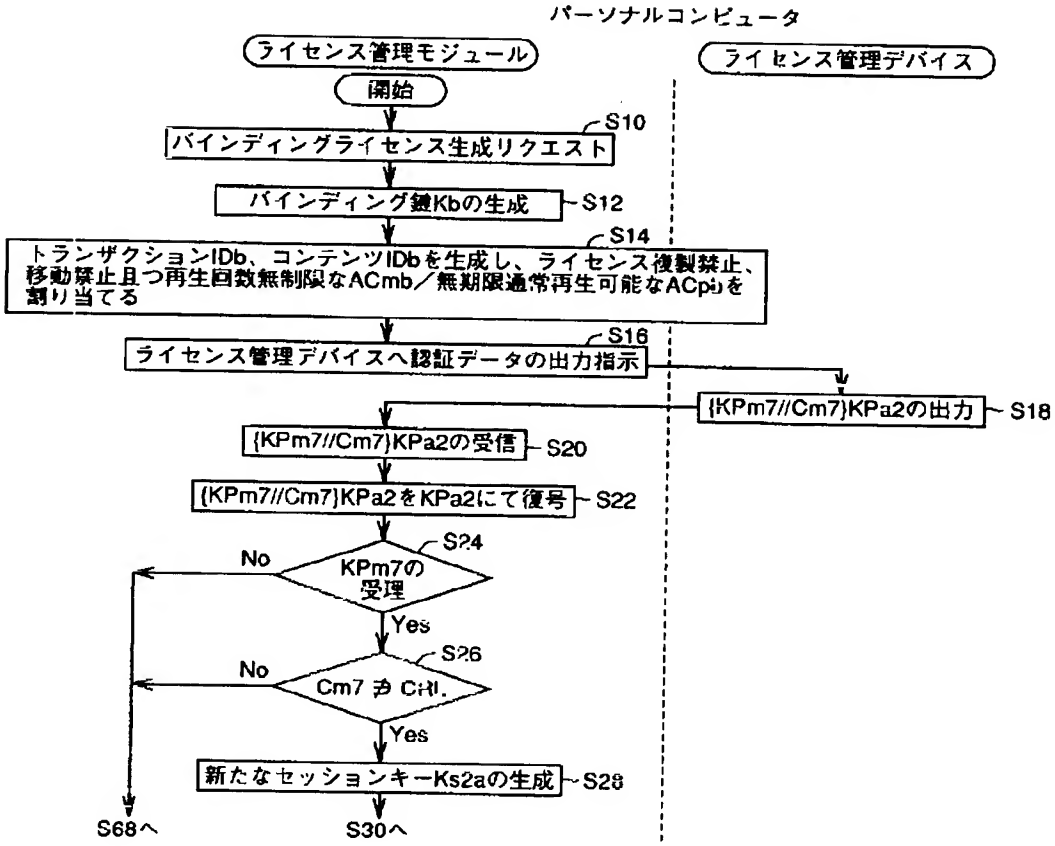
【図8】


110
1400
クラス証明書 {KPm3//Cm3}KPa2
1420
コントローラ
1424
IF
1426
BS4
1415B
1415
1415A
メモリ
CRL
Kc,ACp,ACm, ライセンスID
{Dc}Kc Dc-Inf 再生リストファイル ライセンス管理 ファイル
1415C
1408
1410
1404
1412
1417
1406
1442
1422
復号 KPa
KPpy
KPmx
暗号 KPp/KPm
復号 Kmc
復号 Ks
暗号 KPmc
暗号 Ks
復号 Km
KPa保持
1414
1402
CRL
KPmc4
Ks3
Ks22
1421
Km保持 Km3
Kmc保持 Kmc4
1446
Pb Pa
CRLdate/CRL
Pc
Pd
Pf
Pe
Ks2 発生
Ks2
1418
KPmc保持 KPmc4
1416

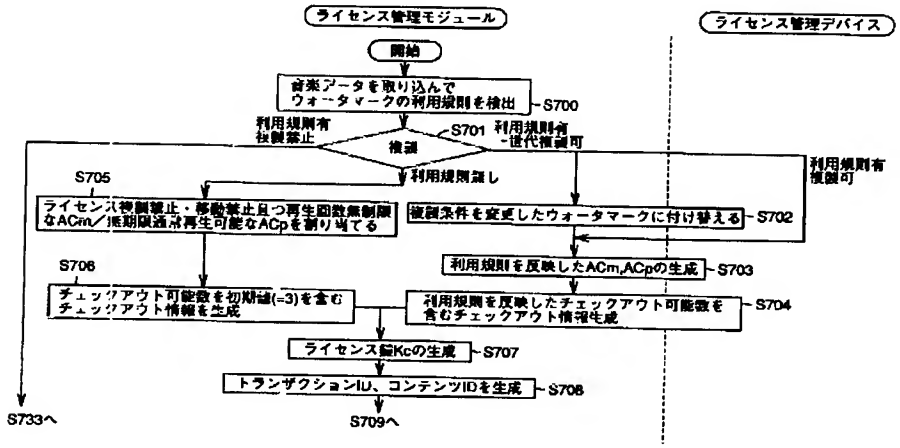
【図9】


520
5200
クラス証明書 {KPm7//Cm7}KPa2
5220
コントローラ
5224
IF
5226
BS5
5215
5215A
メモリ
CRL
Kc,ACp,ACm, ライセンスID
5215B
5208
5210
5204
5212
5217
5206
5242
5222
復号 KPa
KPpy
KPmx
暗号 KPp/KPm
復号 Kmc
復号 Ks
暗号 KPmc
暗号 Ks
復号 Km
KPa保持
5214
5202
CRL
KPmc4
5221
Km保持 Km/
Kmc保持 Kmc8
5246
Pb Pa
CRLdate/CRL
Pc
Pd
Pf
Pe
Ks2 発生
Ks2
5218
KPmc保持 KPmc8
5216

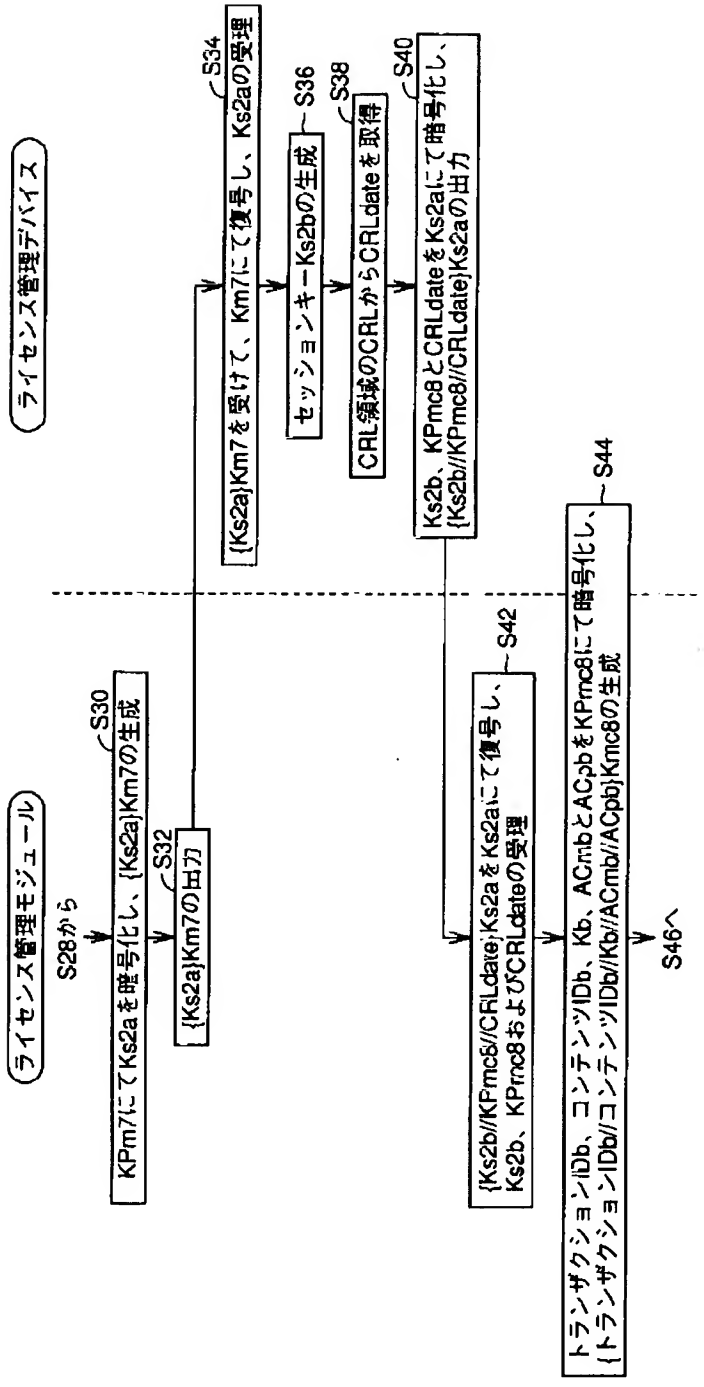
【図10】


パーソナルコンピュータ
ライセンス管理モジュール
ライセンス管理デバイス
開始
S10
バインディングライセンス生成リクエスト
バインディング鍵Kbの生成
S12
S14
トランザクションIDb、コンテンツIDbを生成し、ライセンス複製禁止、移動禁止且つ再生回数無制限なACmb／無期限通常再生可能なACpbを割り当てる
S16
ライセンス管理デバイスへ認証データの出力指示
{KPm7//Cm7}KPa2の出力
S18
{KPm7//Cm7}KPa2の受信
S20
{KPm7//Cm7}KPa2をKPa2にて復号
S22
S24
KPm7の受理
No
Yes
S26
Cm7 = Cm'
No
Yes
新たなセッションキーKs2aの生成
S28
S68へ
S30へ

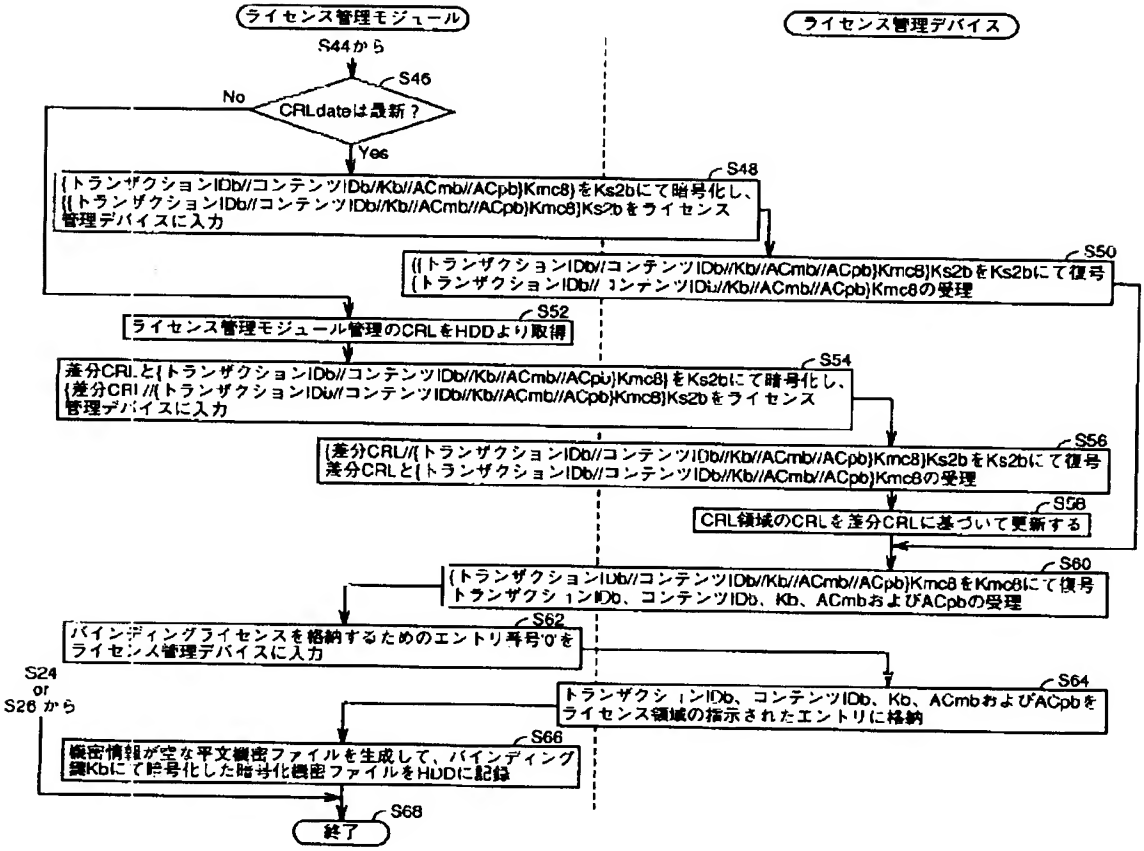
【図22】


ライセンス管理モジュール
ライセンス管理デバイス
開始
音楽データを取り込んでウォータマークの利用規則を検出
S700
利用規則有 複製禁止
検証
S701
利用規則有 一世代複製可
利用規則有 複製可
利用規則無し
S705
ライセンス複製禁止・移動禁止且つ再生回数無制限なACm／無期限通常再生可能なACpを割り当てる
複製条件を変更したウォータマークに付け替える
S702
S706
利用規則を反映したACm,ACpの生成
S703
チェックアウト可能数を初期値(=3)を含むチェックアウト情報を生成
利用規則を反映したチェックアウト可能数を含むチェックアウト情報生成
S704
ライセンス鍵Kcの生成
S707
トランザクションID、コンテンツIDを生成
S708
S733へ
S709へ

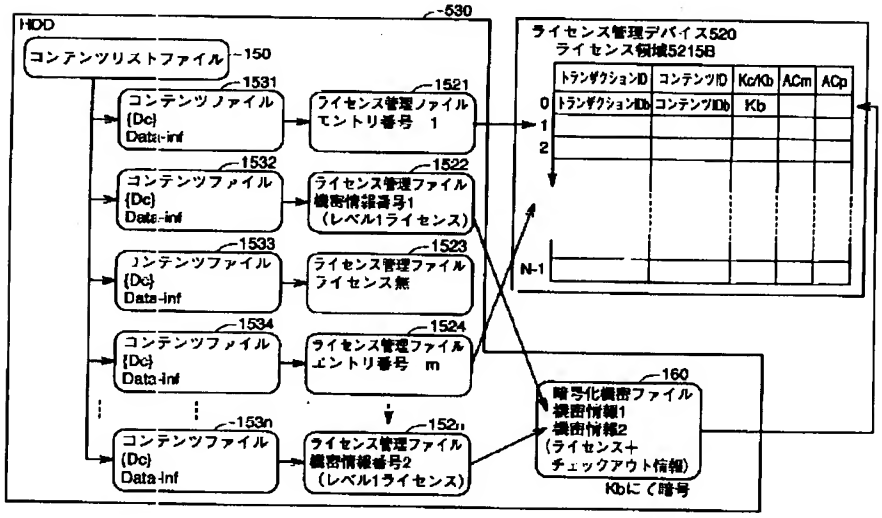
【図11】


ライセンス管理デバイス
ライセンス管理モジュール
S28から
KPm7にてKs2aを暗号化し、{Ks2a}Km7の生成
S30
{Ks2a}Km7の出力
S32
{Ks2a}Km7を受けて、Km7にて復号し、Ks2aの受理
S34
セッションキーKs2bの生成
S36
CRL領域のCRLからCRLdateを取得
S38
Ks2b、KPmc8とCRLdateをKs2aにて暗号化し、{Ks2b//KPmc8//CRLdate}Ks2aの出力
S40
{Ks2b//KPmc8//CRLdate}Ks2aを Ks2aにて復号し、Ks2b、KPmc8およびCRLdateの受理
S42
トランザクションIDb、コンテンツIDb、Kb、ACmbとACpbをKPmc8にて暗号化し、{トランザクションIDb//コンテンツIDb//Kb//ACmb//ACpb}Kmc8の生成
S44
S46へ

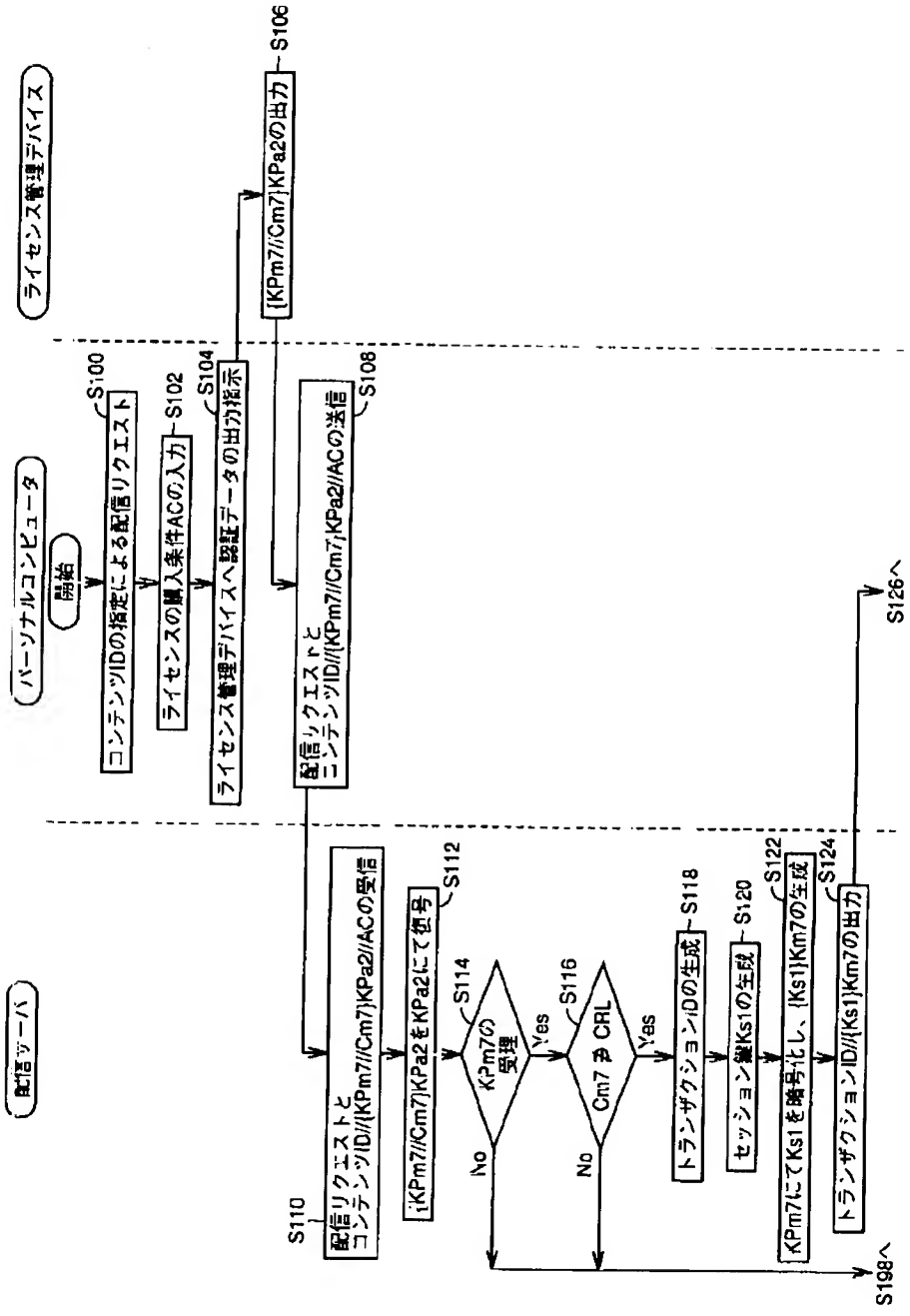
【図12】


ライセンス管理モジュール
ライセンス管理デバイス
S44から
S46
No
CRLdateは最新？
Yes
{トランザクションIDb//コンテンツIDb//Kb//ACmb//ACpb}Kmc8}をKs2bにて暗号化し、{{トランザクションIDb//コンテンツIDb//Kb//ACmb//ACpb}Kmc8}Ks2bをライセンス管理デバイスに入力
S48
{{トランザクションIDb//コンテンツIDb//Kb//ACmb//ACpb}Kmc8}Ks2bをKs2bにて復号{トランザクションIDb//コンテンツIDb//Kb//ACmb//ACpb}Kmc8の受理
S50
ライセンス管理モジュール管理のCRLをHDDより取得
S52
差分CRLと{トランザクションIDb//コンテンツIDb//Kb//ACmb//ACpb}Kmc8}をKs2bにて暗号化し、{差分CRL//{トランザクションIDb//コンテンツIDb//Kb//ACmb//ACpb}Kmc8}Ks2bをライセンス管理デバイスに入力
S54
{差分CRL//{トランザクションIDb//コンテンツIDb//Kb//ACmb//ACpb}Kmc8}Ks2bをKs2bにて復号差分CRLと{トランザクションIDb//コンテンツIDb//Kb//ACmb//ACpb}Kmc8の受理
S56
CRL領域のCRLを差分CRLに基づいて更新する
S58
{トランザクションIDb//コンテンツIDb//Kb//ACmb//ACpb}Kmc8をKmc8にて復号トランザクションIDb、コンテンツIDb、Kb、ACmbおよびACpbの受理
S60
バインディングライセンスを格納するためのエントリ番号'0'をライセンス管理デバイスに入力
S62
S24 or S26から
トランザクションIDb、コンテンツIDb、Kb、ACmbおよびACpbをライセンス領域の指示されたエントリに格納
S64
機密情報が空な平文機密ファイルを生成して、バインディング鍵Kbにて暗号化した暗号化機密ファイルをHDDに記録
S66
終了
S68

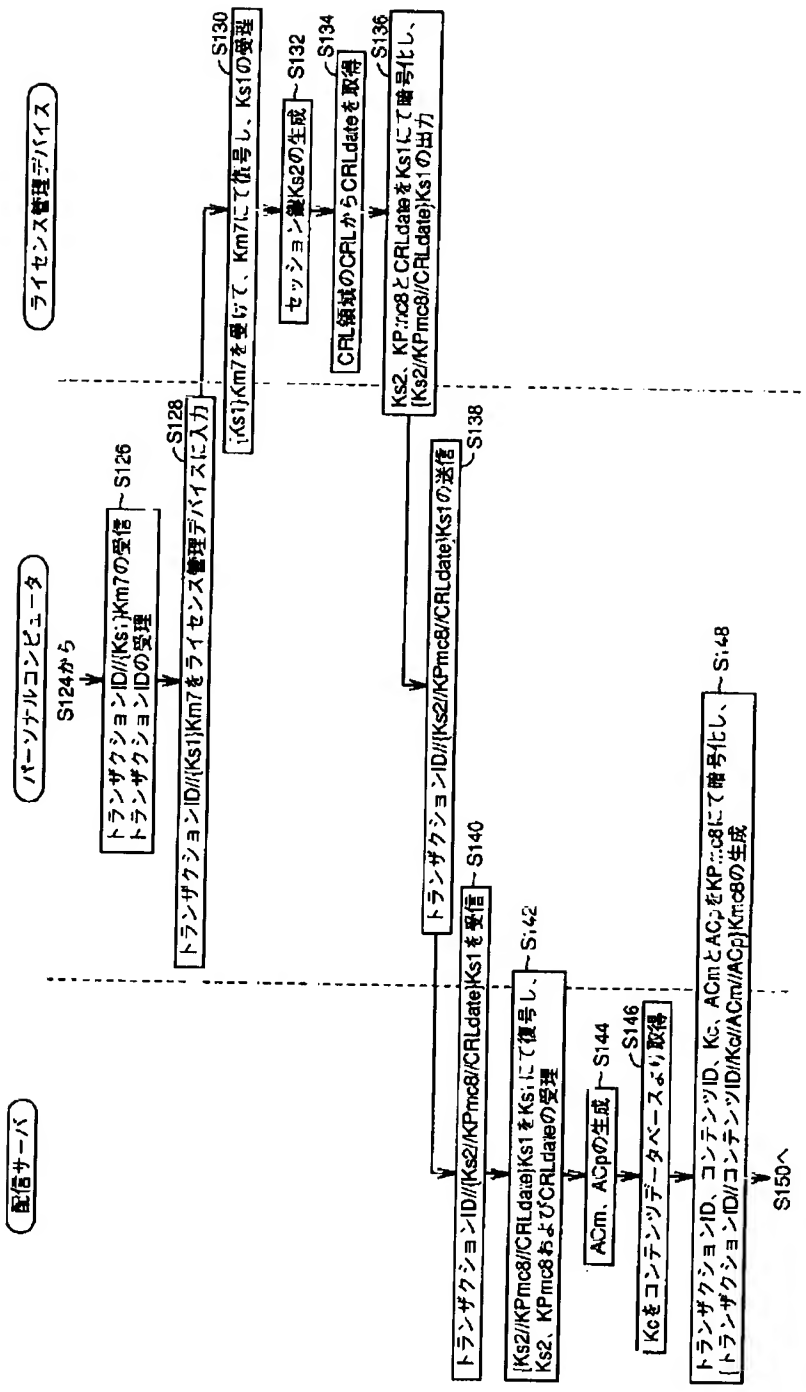
【図25】


HDD
530
コンテンツリストファイル
150
コンテンツファイル {Dc} Data-inf
1531
ライセンス管理ファイル エントリ番号 1
1521
コンテンツファイル {Dc} Data-inf
1532
ライセンス管理ファイル 機密情報番号1 (レベル1ライセンス)
1522
コンテンツファイル {Dc} Data-inf
1533
ライセンス管理ファイル ライセンス無
1523
コンテンツファイル {Dc} Data-inf
1534
ライセンス管理ファイル エントリ番号 m
1524
コンテンツファイル {Dc} Data-inf
153n
ライセンス管理ファイル 機密情報番号2 (レベル1ライセンス)
152n
ライセンス管理デバイス520
ライセンス領域5215B
トランザクションID
コンテンツID
Kc/Kb
ACm
ACp
トランザクションIDb
コンテンツIDb
Kb
0
1
2
N-1
暗号化機密ファイル 機密情報1 機密情報2 (ライセンス+チェックアウト情報) Kbにて暗号
160

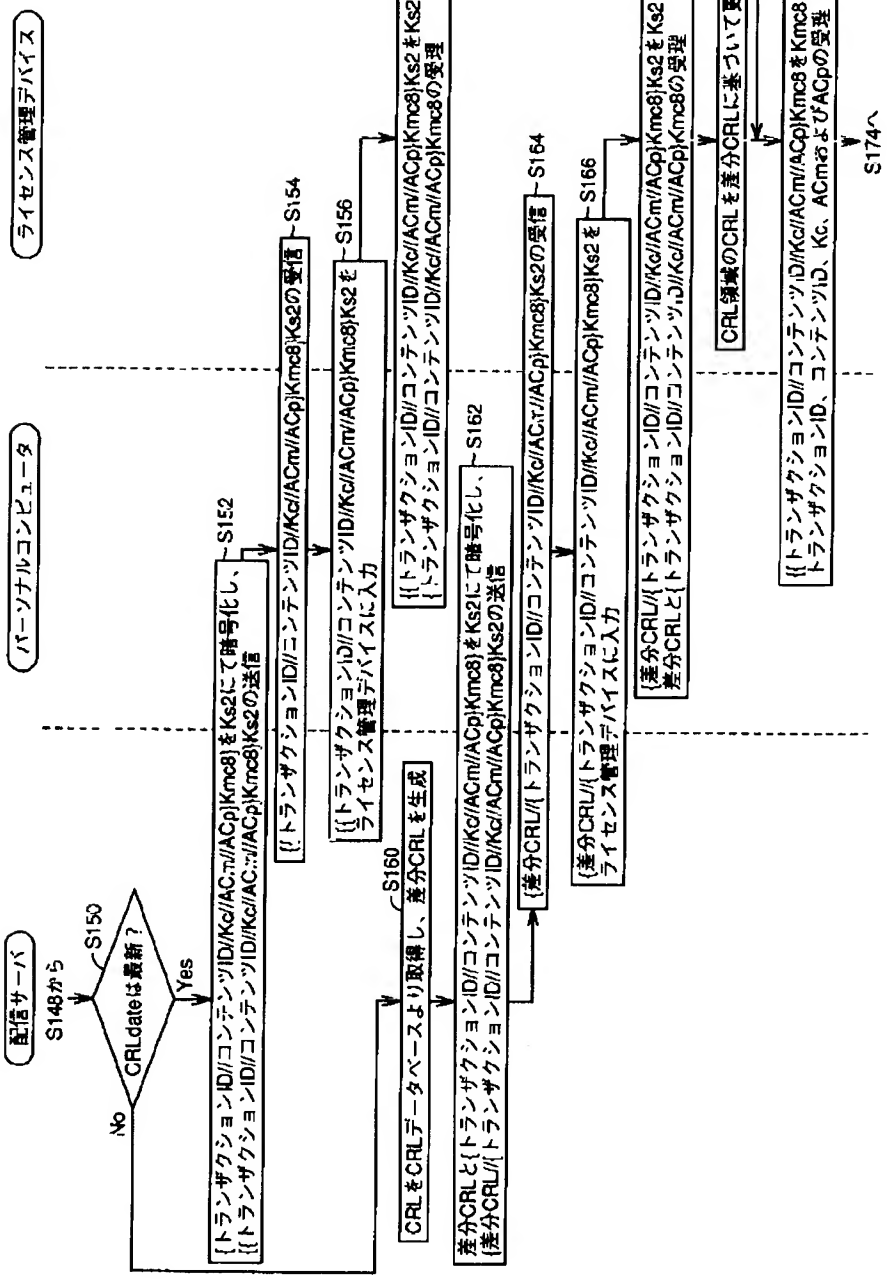
【図13】


ライセンス管理デバイス
パーソナルコンピュータ
配信サーバ
開始
S100
コンテンツIDの指定による配信リクエスト
S102
ライセンスの購入条件ACの入力
S104
ライセンス管理デバイスへ認証データの出力指示
S106
{KPm7//Cm7}KPa2の出力
S108
配信リクエストと
コンテンツID//{KPm7//Cm7;KPa2//ACの送信
S110
配信リクエストと
コンテンツID//{KPm7//Cm7}KPa2//ACの受信
S112
{KPm7//Cm7}KPa2をKPa2にて復号
S114
KPm7の
受理
No
Yes
S116
Cm7 ≠ CRL
No
Yes
S118
トランザクションIDの生成
S120
セッション鍵Ks1の生成
S122
KPm7にてKs1を暗号化し、{Ks1}Km7の生成
S124
トランザクションID//{Ks1}Km7の出力
S126へ
S198へ

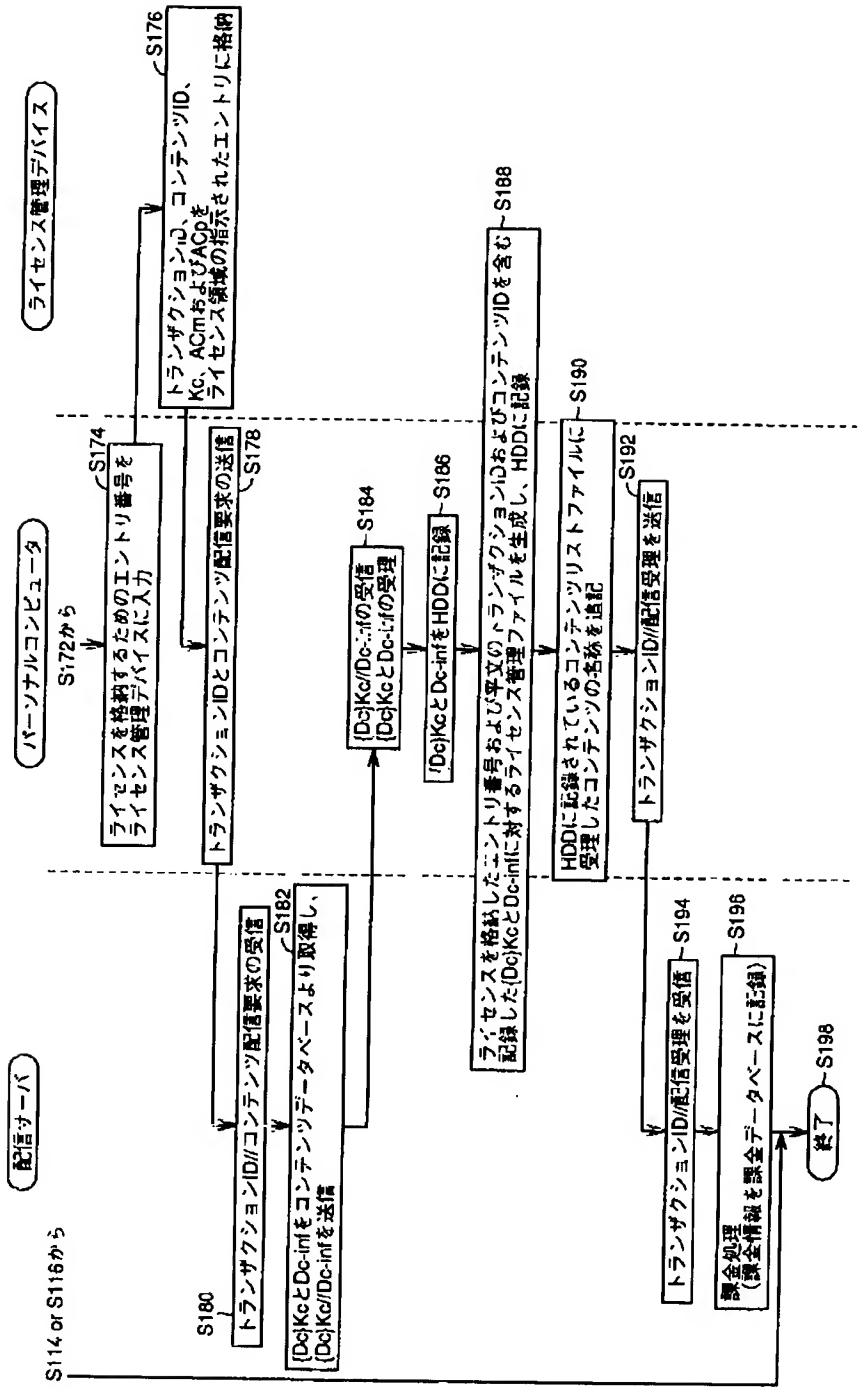
【図14】


配信サーバ
パーソナルコンピュータ
ライセンス管理デバイス
S124から
S126
トランザクションID//{Ks:}Km7の受信
トランザクションIDの受理
S128
トランザクションID//{Ks1}Km7をライセンス管理デバイスに入力
S130
{Ks1}Km7を受けて、Km7にて復号し、Ks1の受理
S132
セッション鍵Ks2の生成
S134
CRL領域のCRLからCRLdateを取得
S136
Ks2、KP::mc8とCRLdateをKs1にて暗号化し、{Ks2//KPmc8//CRLdate}Ks1の出力
S138
トランザクションID//{Ks2//KPmc8//CRLdate}Ks1の送信
S140
トランザクションID//{Ks2//KPmc8//CRLdate}Ks1を受信
S142
{Ks2//KPmc8//CRLdate}Ks1をKs:にて復号し、Ks2、KPmc8およびCRLdateの受理
S144
ACm、ACpの生成
S146
{Kc}をコンテンツデータベースより取得
S148
トランザクションID、コンテンツID、Kc、ACmとACpをKP::c8にて暗号化し、{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8の生成
S150へ

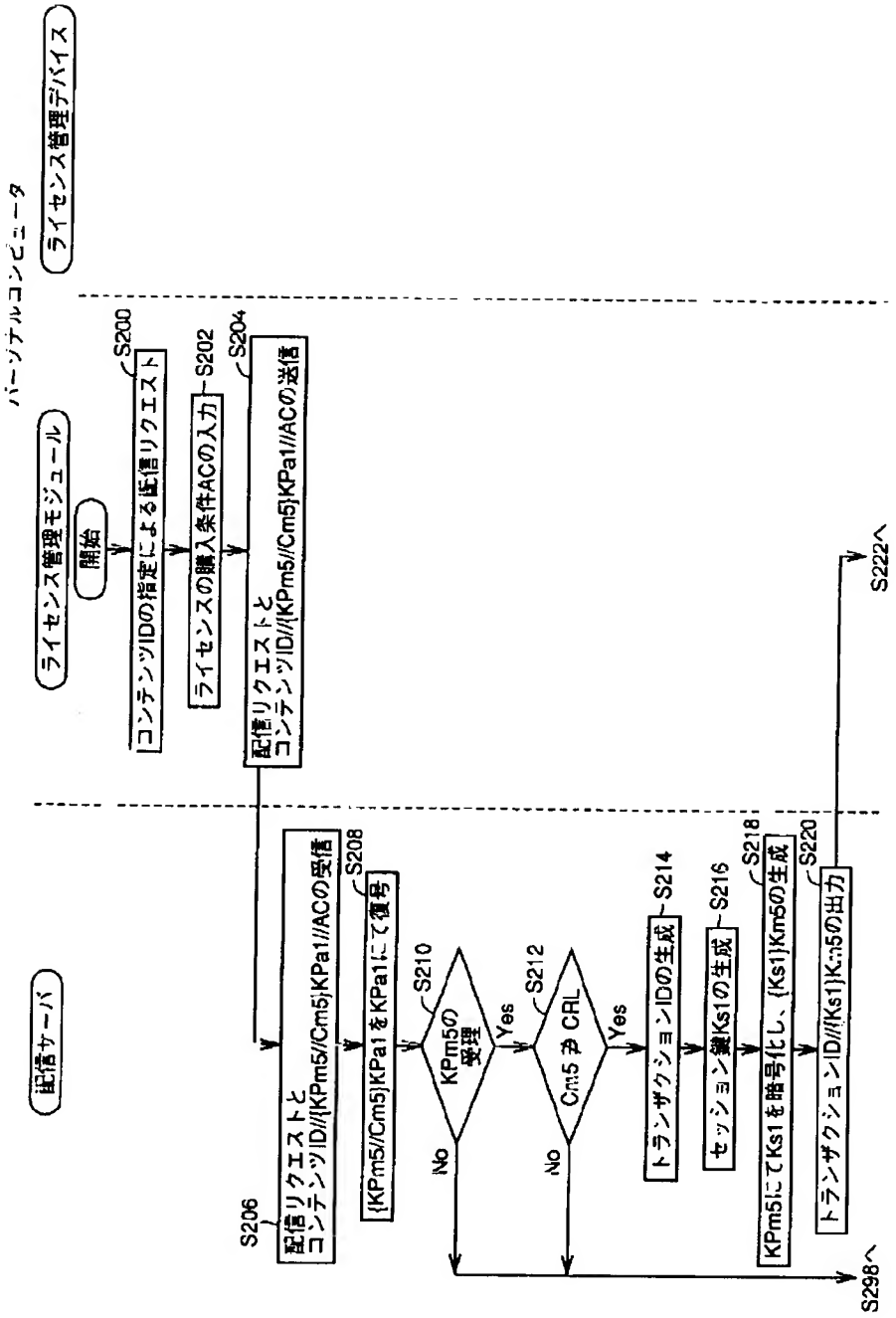
【図15】


配信サーバ
パーソナルコンピュータ
ライセンス管理デバイス
S148から
S150
CRLdateは最新？
No
Yes
{{トランザクションID//コンテンツID//Kc//AC::n//ACp}Kmc8}をKs2にて暗号化し、
{{トランザクションID//コンテンツID//Kc//AC::n//ACp}Kmc8}Ks2の送信
S152
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8}Ks2の受信
S154
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8}Ks2を
ライセンス管理デバイスに入力
S156
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8}Ks2をKs2にて復号
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8の受理
S158
CRLをCRLデータベースより取得し、差分CRLを生成
S160
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8}をKs2にて暗号化し、
S162
差分CRLと{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8}Ks2の送信
{差分CRL//{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8}Ks2の受信
S164
{差分CRL//{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8}Ks2を
ライセンス管理デバイスに入力
S166
{差分CRL//{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8}Ks2をKs2にて復号
差分CRLと{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8の受理
S168
CRL領域のCRLを差分CRLに基づいて更新する
S170
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc8をKmc8にて復号
トランザクションID、コンテンツID、Kc、ACmおよびACpの受理
S172
S174へ

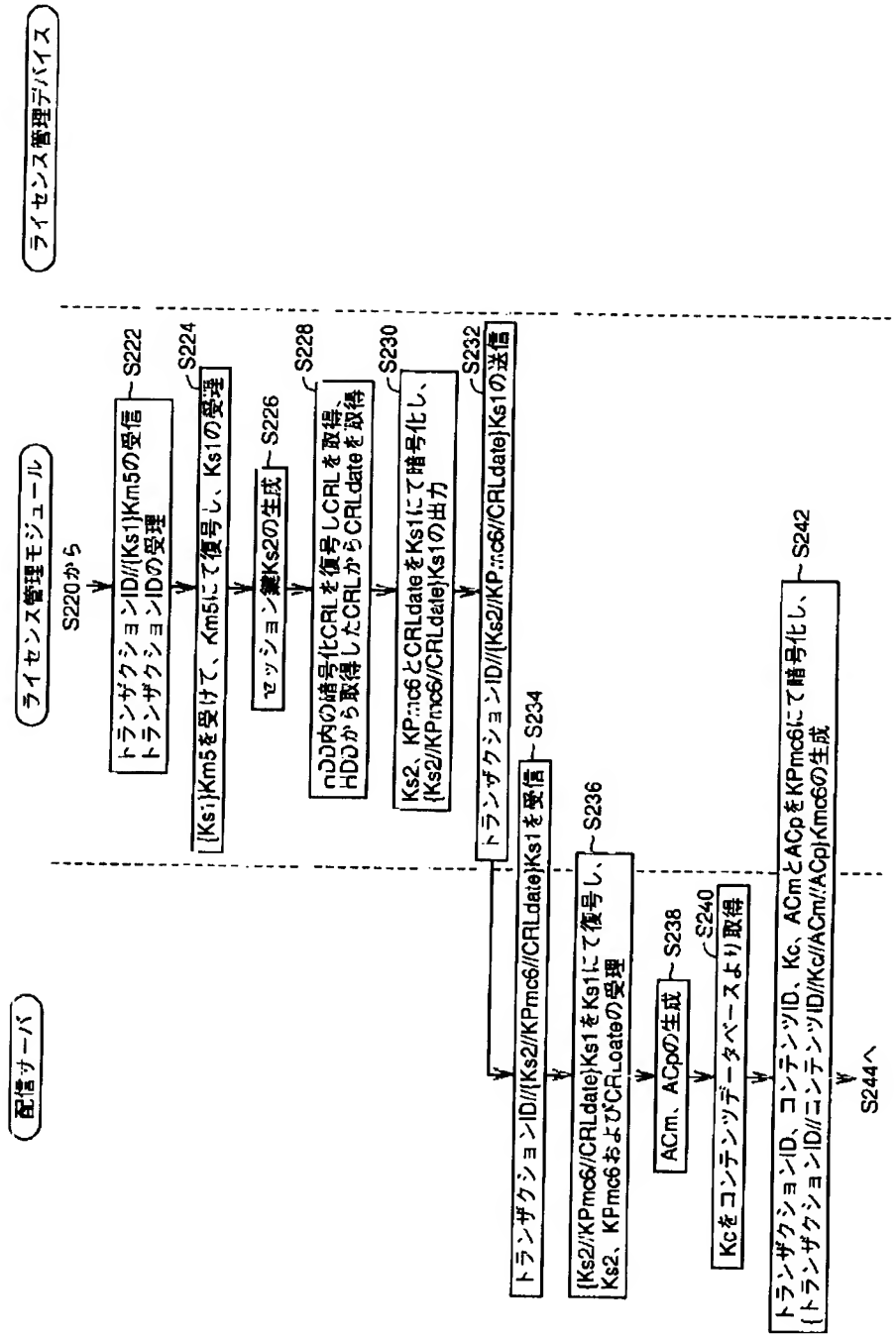
【図16】


ライセンス管理デバイス
パーソナルコンピュータ
配信サーバ
S172から
ライセンスを格納するためのエントリ番号をライセンス管理デバイスに入力
S174
トランザクションIDとコンテンツ配信要求の送信
S178
トランザクションID、コンテンツID、Kc、ACmおよびACpをライセンス領域の指示されたエントリに格納
S176
トランザクションID//コンテンツ配信要求の受信
S180
{Dc}Kc//Dc-infの受信
{Dc}KcとDc-infの受理
S184
{Dc}Kc//Dc-infをコンテンツデータベースより取得し、{Dc}Kc//Dc-infを送信
S182
{Dc}KcとDc-infをHDDに記録
S186
ライセンスを格納したエントリ番号および平文のトランザクションIDおよびコンテンツIDを含む記録した{Dc}KcとDc-infに対するライセンス管理ファイルを生成し、HDDに記録
S188
HDDに記録されているコンテンツリストファイルに受理したコンテンツの名称を追記
S190
トランザクションID//配信受理を送信
S192
トランザクションID//配信受理を受信
S194
課金処理（課金情報を課金データベースに記録）
S196
終了
S198
S114 or S116から

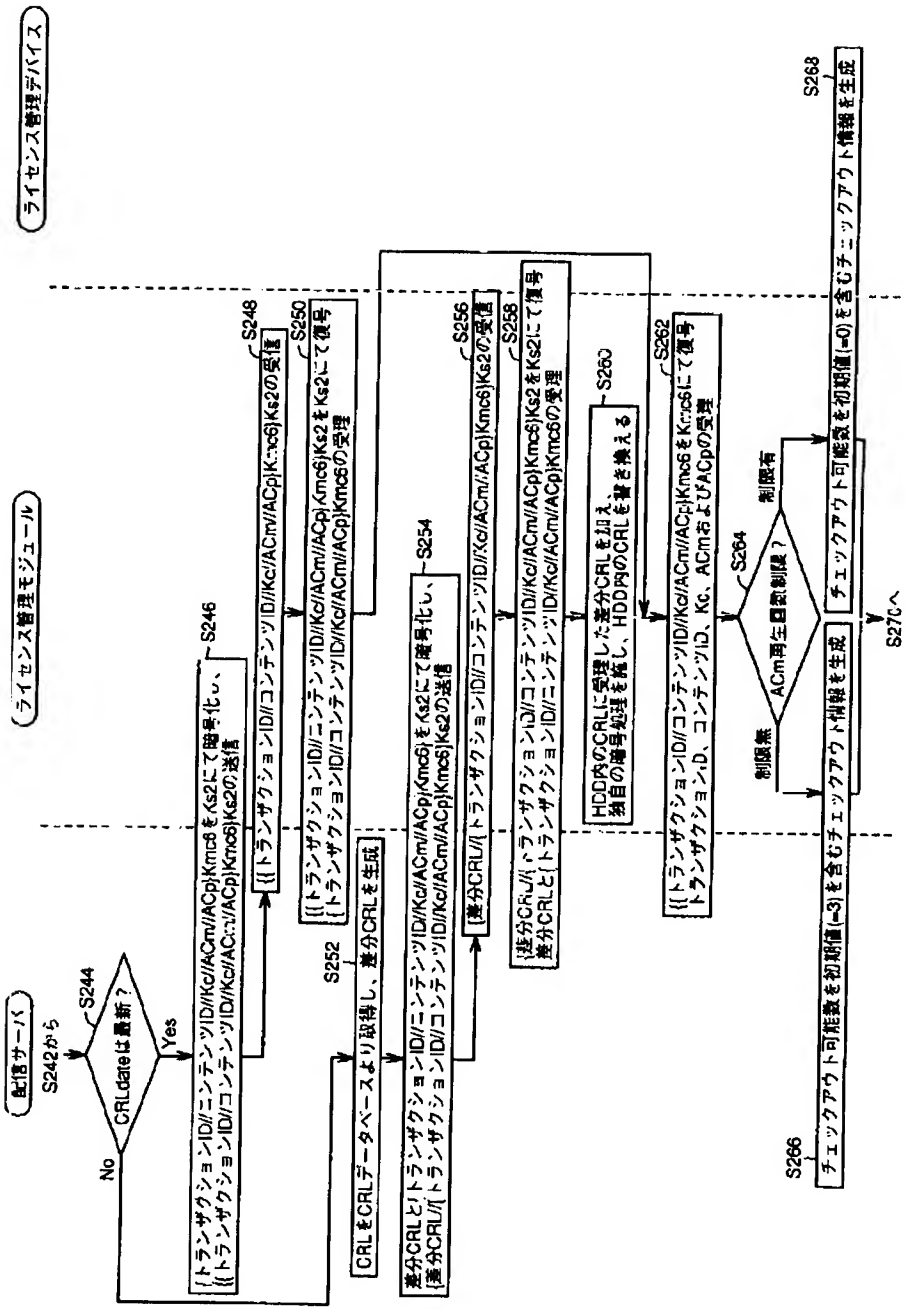
【図17】


パーソナルコンピュータ
ライセンス管理デバイス
ライセンス管理モジュール
開始
S200
コンテンツIDの指定による配信リクエスト
S202
ライセンスの購入条件ACの入力
S204
配信リクエストと
コンテンツID//{KPm5//Cm5}KPa1//ACの送信
配信サーバ
S206
配信リクエストと
コンテンツID//{KPm5//Cm5}KPa1//ACの受信
S208
{KPm5//Cm5}KPa1をKPa1にて復号
S210
KPm5の
受理
No
Yes
S212
Cm5 が CRL
No
Yes
S214
トランザクションIDの生成
S216
セッション鍵Ks1の生成
S218
KPm5にてKs1を暗号化し、{Ks1}Km5の生成
S220
トランザクションID//{Ks1}Km5の出力
S222へ
S298へ

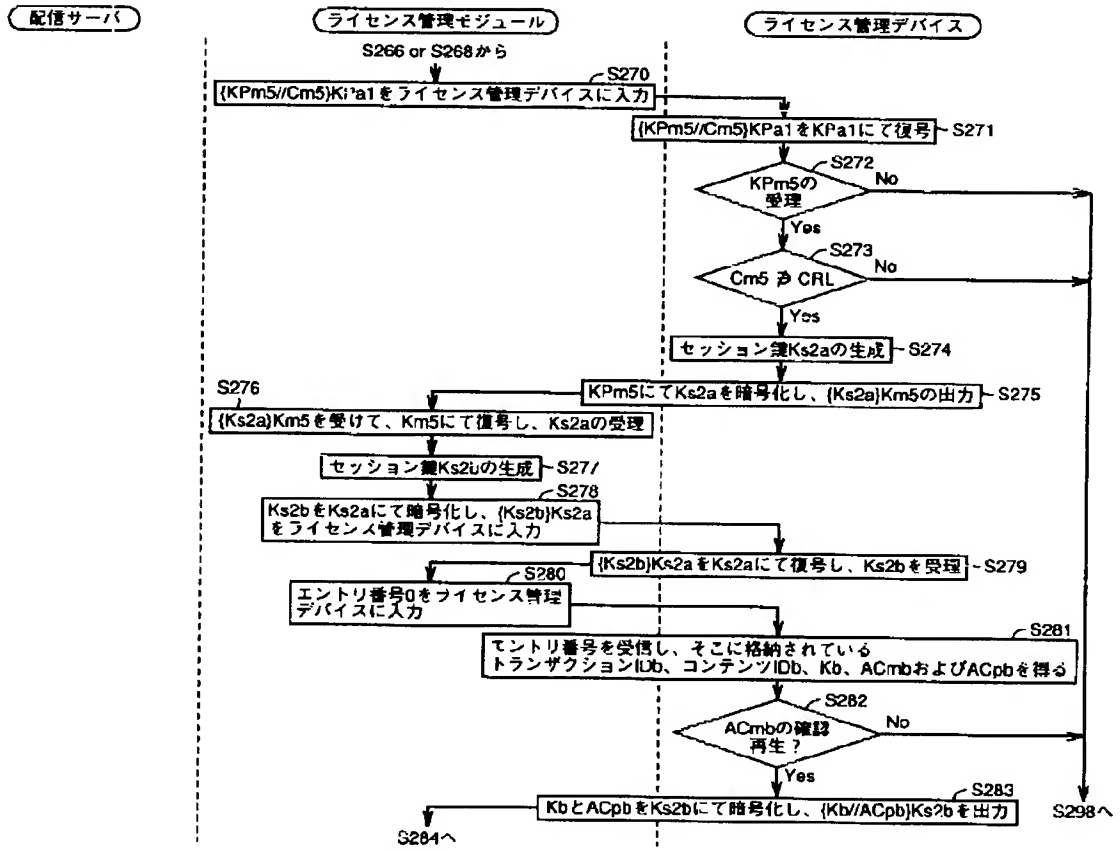
【図18】


ライセンス管理デバイス
ライセンス管理モジュール
配信サーバ
S220から
トランザクションID//{Ks1}Km5の受信
トランザクションIDの受理
S222
S224
{Ks1}Km5を受けて、Km5にて復号し、Ks1の受理
S226
セッション鍵Ks2の生成
S228
nDD内の暗号化CRLを復号しCRLを取得、
HDDから取得したCRLからCRLdateを取得
S230
Ks2、KPmc6とCRLdateをKs1にて暗号化し、
{Ks2//KPmc6//CRLdate}Ks1の出力
S232
トランザクションID//{Ks2//KPmc6//CRLdate}Ks1の送信
トランザクションID//{Ks2//KPmc6//CRLdate}Ks1を受信
S234
{Ks2//KPmc6//CRLdate}Ks1をKs1にて復号し、
Ks2、KPmc6およびCRLoateの受理
S236
ACm、ACpの生成
S238
Kcをコンテンツデータベースより取得
S240
トランザクションID、コンテンツID、Kc、ACmとACpをKPmc6にて暗号化し、
{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc6の生成
S242
S244へ

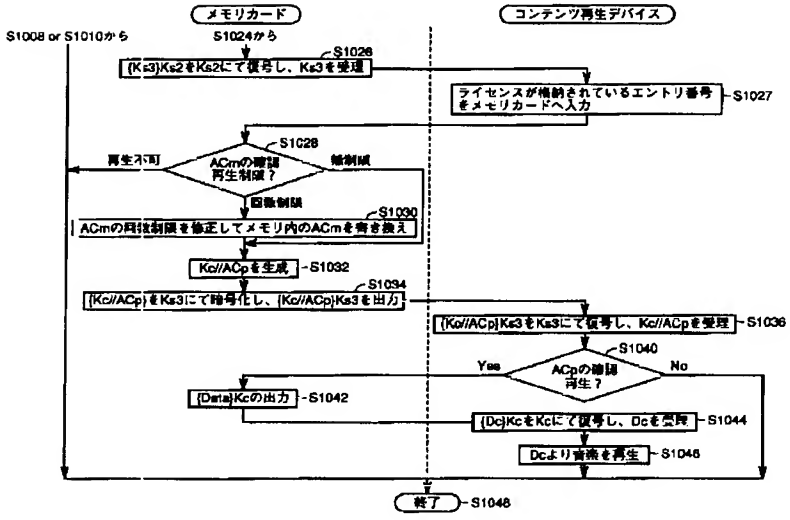
【図19】


配信サーバ
ライセンス管理モジュール
ライセンス管理デバイス
S242から
S244
CRLdateは最新？
No
Yes
{{トランザクションID//ニンテンツID//Kc//ACm//ACp}Kmc6をKs2にて暗号化し、
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc6}Ks2の送信
S246
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc6}Ks2の受信
S248
{{トランザクションID//ニンテンツID//Kc//ACm//ACp}Kmc6}Ks2をKs2にて復号
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc6の受理
S250
CRLをCRLデータベースより取得し、差分CRLを生成
S252
差分CRLと{トランザクションID//ニンテンツID//Kc//ACm//ACp}Kmc6}をKs2にて暗号化し、
{差分CRL//{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc6}Ks2の送信
S254
{差分CRL//{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc6}Ks2の受信
S256
{差分CRL//{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc6}Ks2をKs2にて復号
差分CRLと{トランザクションID//ニンテンツID//Kc//ACm//ACp}Kmc6の受理
S258
HDD内のCRLに受理した差分CRLを加え、
独自の暗号処理を施し、HDD内のCRLを皆を換える
S260
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc6をKmc6にて復号
トランザクションID、コンテンツID、Kc、ACmおよびACpの受理
S262
ACm再生回数制限？
S264
制限有
制限無
チェックアウト可能数を初期値(=0)を含むチェックアウト情報を生成
S268
チェックアウト可能数を初期値(=3)を含むチェックアウト情報を生成
S266
S270へ

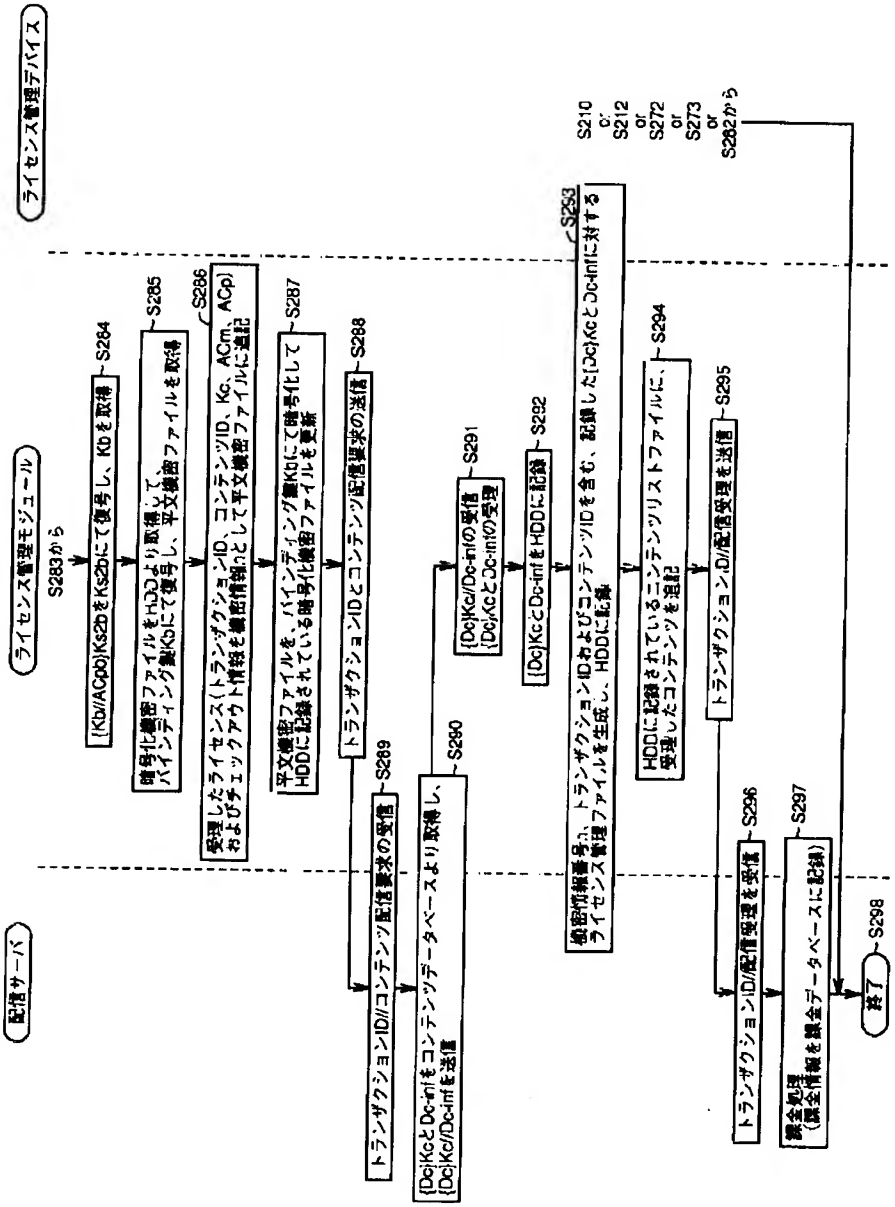
【図20】


配信サーバ
ライセンス管理モジュール
ライセンス管理デバイス
S266 or S268から
S270
{KPm5//Cm5}Ki'a1をライセンス管理デバイスに入力
{KPm5//Cm5}KPa1をKPa1にて復号
S271
S272
KPm5の受理
No
Yes
S273
Cm5 ≠ CRL
No
Yes
セッション鍵Ks2aの生成
S274
S276
KPm5にてKs2aを暗号化し、{Ks2a}Km5の出力
S275
{Ks2a}Km5を受けて、Km5にて復号し、Ks2aの受理
セッション鍵Ks2bの生成
S277
S278
Ks2bをKs2aにて暗号化し、{Ks2b}Ks2aをライセンス管理デバイスに入力
{Ks2b}Ks2aをKs2aにて復号し、Ks2bを受理
S279
S280
エントリ番号0をライセンス管理デバイスに入力
S281
エントリ番号を受信し、そこに格納されているトランザクションIDb、コンテンツIDb、Kb、ACmbおよびACpbを得る
S282
ACmbの確認再生？
No
Yes
S283
KbとACpbをKs2bにて暗号化し、{Kb//ACpb}Ks2bを出力
S298へ
S284へ

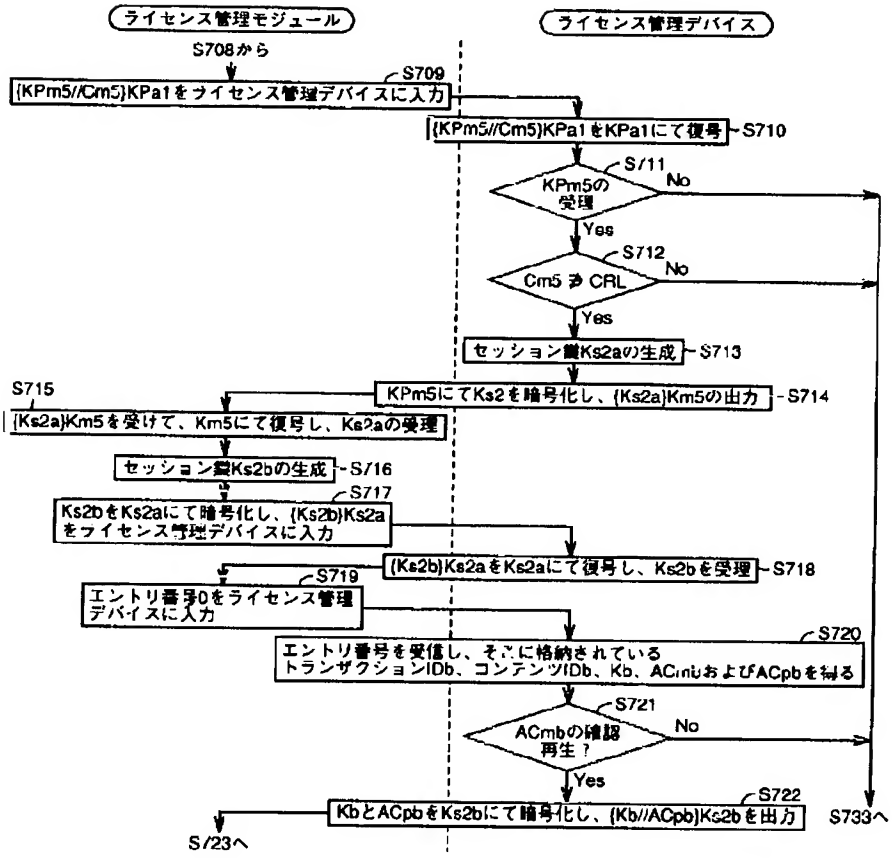
【図40】


メモリカード
コンテンツ再生デバイス
S1008 or S1010から
S1024から
S1026
{Ks3}Ks2をKs2にて復号し、Ks3を受理
ライセンスが格納されているエントリ番号をメモリカードへ入力
S1027
S1028
ACmの確認再生制限？
再生不可
無制限
回数制限
S1030
ACmの再生制限を修正してメモリ内のACmを書き換え
Kc//ACpを生成
S1032
S1034
{Kc//ACp}をKs3にて暗号化し、{Kc//ACp}Ks3を出力
{Kc//ACp}Ks3をKs3にて復号し、Kc//ACpを受理
S1036
S1040
ACpの確認再生？
Yes
No
{Data}Kcの出力
S1042
{Dc}KcをKcにて復号し、Dcを受理
S1044
Dcより音楽を再生
S1046
終了
S1048

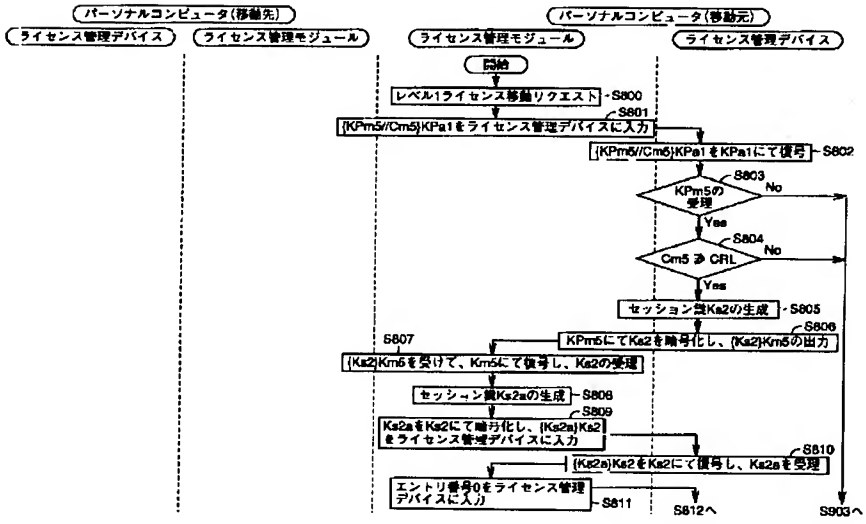
【図21】


ライセンス管理デバイス
ライセンス管理モジュール
配信サーバ
S283から
{Kb//ACpb}Ks2bをKs2bにて復号し、Kbを取得
S284
暗号化機密ファイルをHDDより取得して、
バインディング鍵Kbにて復号し、平文機密ファイルを取得
S285
受理したライセンス(トランザクションID、コンテンツID、Kg、ACm、ACp)
およびチェックアウト情報を機密情報nとして平文機密ファイルに追記
S286
平文機密ファイルを、バインディング鍵Kbにて暗号化して
HDDに記録されている暗号化機密ファイルを更新
S287
トランザクションIDとコンテンツ配信要求の送信
S288
トランザクションID//コンテンツ配信要求の受信
S289
{Dc}KcとDc-infをコンテンツデータベースより取得し、
{Dc}Kc//Dc-infを送信
S290
{Dc}Kc//Dc-infの受信
{Dc}KcとDc-infの受理
S291
{Dc}KcとDc-infをHDDに記録
S292
機密情報番号n、トランザクションIDおよびコンテンツIDを含む、記録した{Dc}KcとDc-infに対する
ライセンス管理ファイルを生成し、HDDに記録
S293
S210
or
S212
or
S272
or
S273
or
S282から
HDDに記録されているコンテンツリストファイルに、
受理したコンテンツを追記
S294
トランザクションID/配信受理を送信
S295
トランザクションID/配信受理を受信
S296
課金処理
(課金情報を課金データベースに記録)
S297
終了
S298

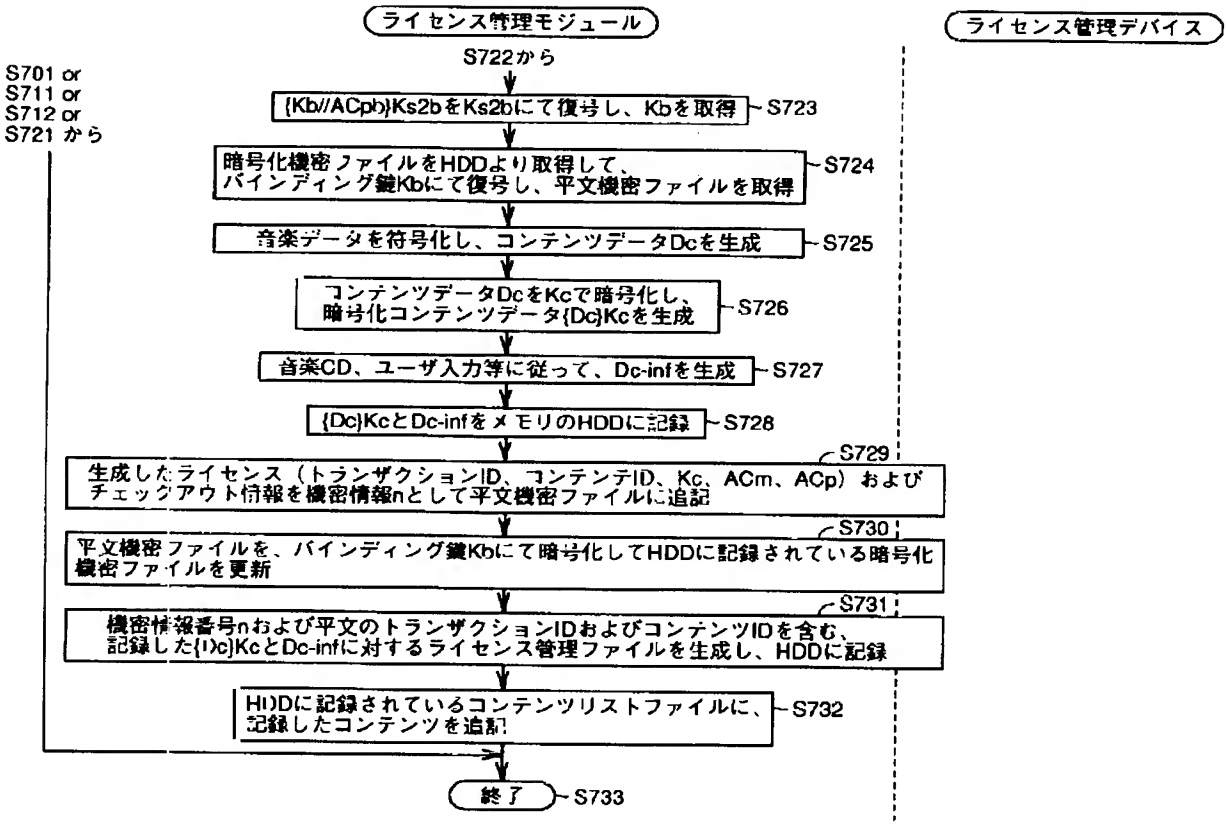
【図２３】


ライセンス管理モジュール
ライセンス管理デバイス
S708から
S709
{KPm5//Cm5}KPa1をライセンス管理デバイスに入力
{KPm5//Cm5}KPa1をKPa1にて復号
S710
S711
KPm5の受理
No
Yes
S712
Cm5 ∋ CRL
No
Yes
セッション鍵Ks2aの生成
S713
S715
KPm5にてKs2を暗号化し、{Ks2a}Km5の出力
S714
{Ks2a}Km5を受けて、Km5にて復号し、Ks2aの受理
セッション鍵Ks2bの生成
S716
S717
Ks2bをKs2aにて暗号化し、{Ks2b}Ks2a
をライセンス管理デバイスに入力
{Ks2b}Ks2aをKs2aにて復号し、Ks2bを受理
S718
S719
エントリ番号0をライセンス管理
デバイスに入力
S720
エントリ番号を受信し、それに格納されている
トランザクションIDb、コンテンツIDb、Kb、ACmbおよびACpbを得る
S721
ACmbの確認
再生？
No
Yes
S722
KbとACpbをKs2bにて暗号化し、{Kb//ACpb}Ks2bを出力
S733へ
S723へ

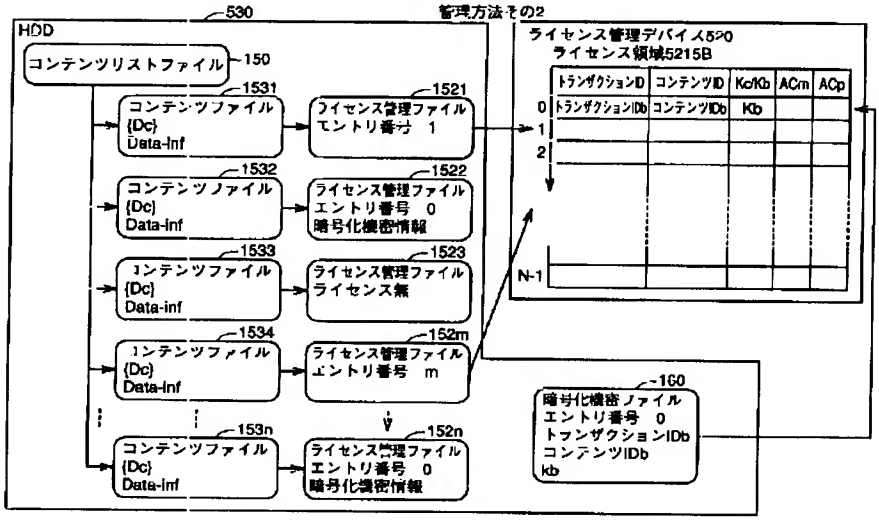
【図４１】


パーソナルコンピュータ(移動先)
ライセンス管理デバイス
ライセンス管理モジュール
パーソナルコンピュータ(移動元)
ライセンス管理モジュール
ライセンス管理デバイス
開始
レベル1ライセンス移動リクエスト
S800
S801
{KPm5//Cm5}KPa1をライセンス管理デバイスに入力
{KPm5//Cm5}KPa1をKPa1にて復号
S802
S803
KPm5の受理
No
Yes
S804
Cm5 ∋ CRL
No
Yes
セッション鍵Ks2の生成
S805
S806
KPm5にてKs2を暗号化し、{Ks2}Km5の出力
S807
{Ks2}Km5を受けて、Km5にて復号し、Ks2の受理
セッション鍵Ks2aの生成
S808
S809
Ks2aをKs2にて暗号化し、{Ks2a}Ks2
をライセンス管理デバイスに入力
S810
{Ks2a}Ks2をKs2にて復号し、Ks2aを受理
エントリ番号0をライセンス管理
デバイスに入力
S811
S812へ
S903へ

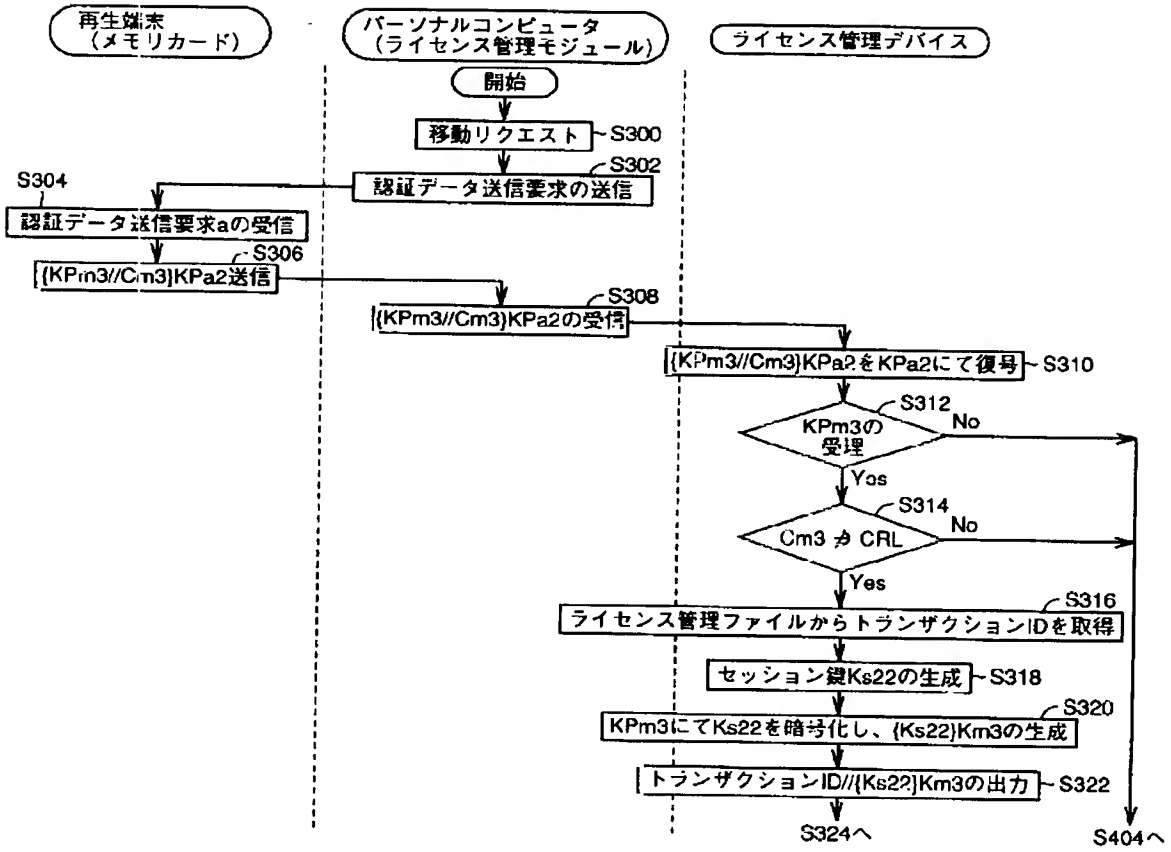
【図24】


ライセンス管理モジュール
ライセンス管理デバイス
S722から
S701 or
S711 or
S712 or
S721 から
{Kb//ACpb}Ks2bをKs2bにて復号し、Kbを取得
S723
暗号化機密ファイルをHDDより取得して、
バインディング鍵Kbにて復号し、平文機密ファイルを取得
S724
音楽データを符号化し、コンテンツデータDcを生成
S725
コンテンツデータDcをKcで暗号化し、
暗号化コンテンツデータ{Dc}Kcを生成
S726
音楽CD、ユーザ入力等に従って、Dc-infを生成
S727
{Dc}KcとDc-infをメモリのHDDに記録
S728
S729
生成したライセンス（トランザクションID、コンテンテID、Kc、ACm、ACp）および
チェックアウト情報を機密情報nとして平文機密ファイルに追記
S730
平文機密ファイルを、バインディング鍵Kbにて暗号化してHDDに記録されている暗号化
機密ファイルを更新
S731
機密情報番号nおよび平文のトランザクションIDおよびコンテンツIDを含む、
記録した{Dc}KcとDc-infに対するライセンス管理ファイルを生成し、HDDに記録
HDDに記録されているコンテンツリストファイルに、
記録したコンテンツを追記
S732
終了
S733

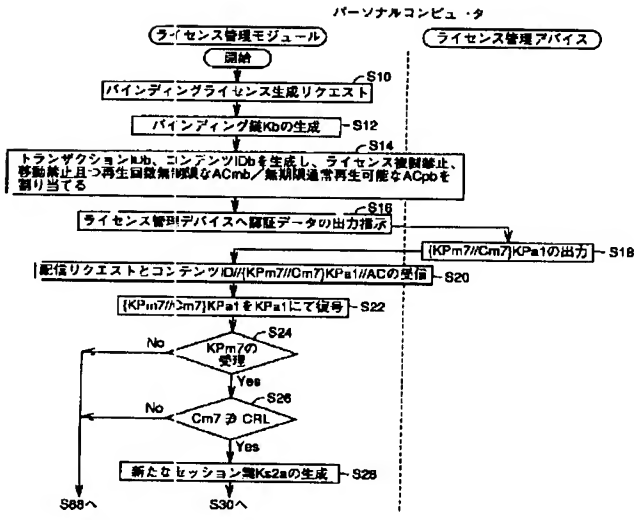
【図49】


530
管理方法その2
HDD
コンテンツリストファイル
150
1531
コンテンツファイル
{Dc}
Data-inf
1521
ライセンス管理ファイル
エントリ番号 1
1532
コンテンツファイル
{Dc}
Data-inf
1522
ライセンス管理ファイル
エントリ番号 0
暗号化機密情報
1533
コンテンツファイル
{Dc}
Data-inf
1523
ライセンス管理ファイル
ライセンス無
1534
コンテンツファイル
{Dc}
Data-inf
152m
ライセンス管理ファイル
エントリ番号 m
153n
コンテンツファイル
{Dc}
Data-inf
152n
ライセンス管理ファイル
エントリ番号 0
暗号化機密情報
ライセンス管理デバイス520
ライセンス領域5215B
トランザクションID
コンテンツID
Kc/Kb
ACm
ACp
0
トランザクションIDb
コンテンツIDb
Kb
1
2
N-1
160
暗号化機密ファイル
エントリ番号 0
トランザクションIDb
コンテンツIDb
kb

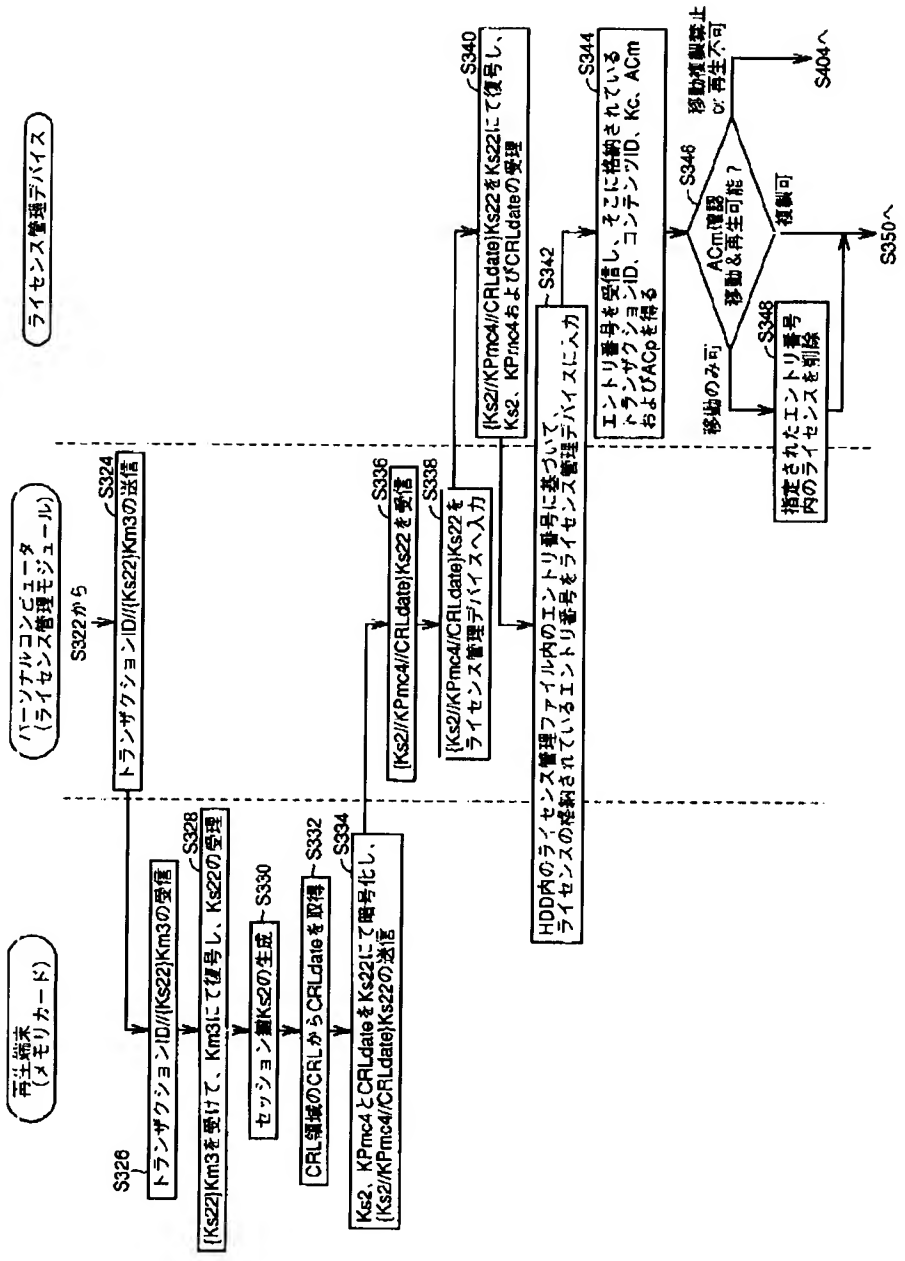
【図26】


再生端末
(メモリカード)
パーソナルコンピュータ
(ライセンス管理モジュール)
ライセンス管理デバイス
開始
移動リクエスト
S300
S302
認証データ送信要求の送信
S304
認証データ送信要求aの受信
S306
{KPm3//Cm3}KPa2送信
S308
{KPm3//Cm3}KPa2の受信
{KPm3//Cm3}KPa2をKPa2にて復号
S310
S312
KPm3の受理
No
Yes
S314
Cm3 ≠ CRL
No
Yes
S316
ライセンス管理ファイルからトランザクションIDを取得
セッション鍵Ks22の生成
S318
S320
KPm3にてKs22を暗号化し、{Ks22}Km3の生成
トランザクションID//{Ks22}Km3の出力
S322
S324へ
S404へ

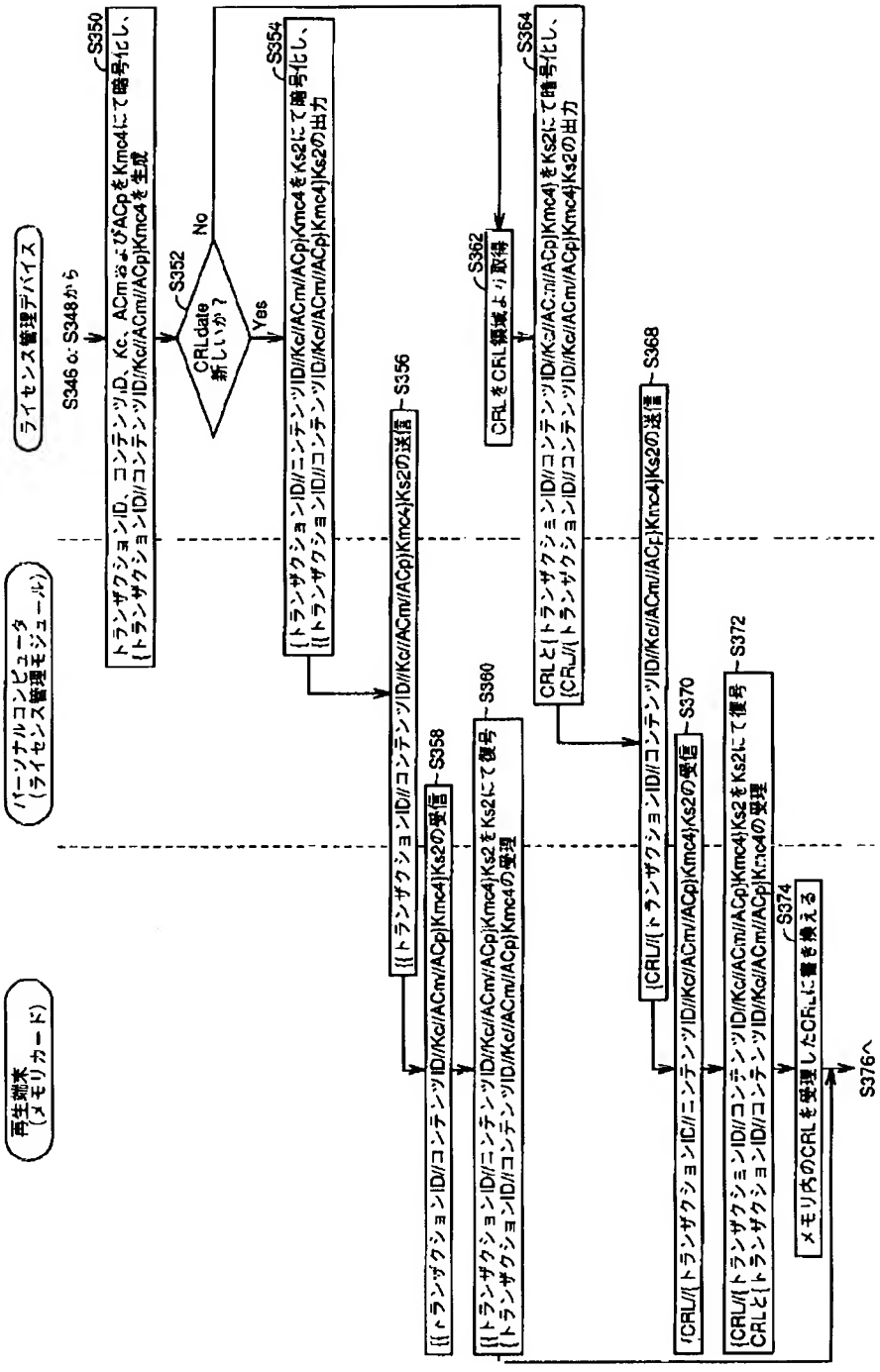
【図50】


パーソナルコンピュータ
ライセンス管理モジュール
ライセンス管理デバイス
開始
S10
バインディングライセンス生成リクエスト
バインディング鍵Kbの生成
S12
S14
トランザクションIDb、コンテンツIDbを生成し、ライセンス複製禁止、
移動禁止且つ再生回数無制限なACmb／無期限通常再生可能なACpbを
割り当てる
S16
ライセンス管理デバイスへ認証データの出力指示
{KPm7//Cm7}KPa1の出力
S18
配信リクエストとコンテンツID//{KPm7//Cm7}KPa1//ACの受信
S20
{KPm7//Cm7}KPa1をKPa1にて復号
S22
S24
No
KPm7の受理
Yes
S26
No
Cm7 ≠ CRL
Yes
新たなセッション鍵Ks2aの生成
S28
S68へ
S30へ

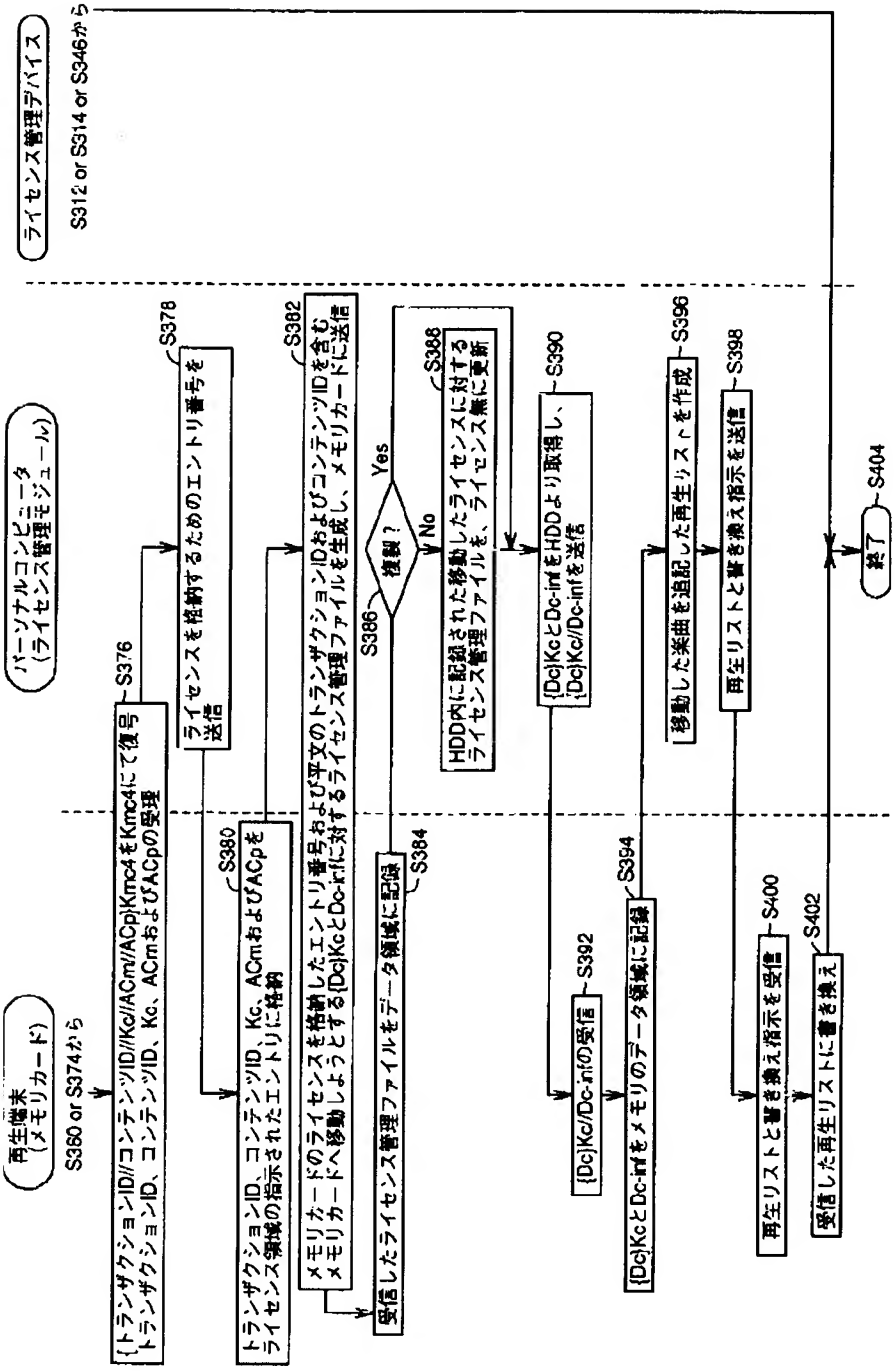
【図27】


再生端末
(メモリカード)
パーソナルコンピュータ
(ライセンス管理モジュール)
ライセンス管理デバイス
S322から
S324
トランザクションID//{Ks22}Km3の送信
S326
トランザクションID//{Ks22}Km3の受信
S328
{Ks22}Km3を受けて、Km3にて復号し、Ks22の受理
S330
セッション鍵Ks20の生成
S332
CRL領域のCRLからCRLdateを取得
S334
Ks2、KPmc4とCRLdateをKs22にて暗号化し、
{Ks2//KPmc4//CRLdate}Ks22の送信
S336
{Ks2//KPmc4//CRLdate}Ks22を受信
S338
{Ks2//KPmc4//CRLdate}Ks22を
ライセンス管理デバイスへ入力
S340
{Ks2//KPmc4//CRLdate}Ks22をKs22にて復号し、
Ks2、KPmc4およびCRLdateの受理
S342
HDD内のライセンス管理ファイル内のエントリ番号に基づいて、
ライセンスの格納されているエントリ番号をライセンス管理デバイスに入力
S344
エントリ番号を受信し、そこに格納されている
トランザクションID、コンテンツID、Kc、ACm
およびACpを得る
S346
ACm確認
移動&再生可能？
移動のみ可
移動複製禁止
or 再生不可
複製可
S348
指定されたエントリ番号
内のライセンスを削除
S350へ
S404へ

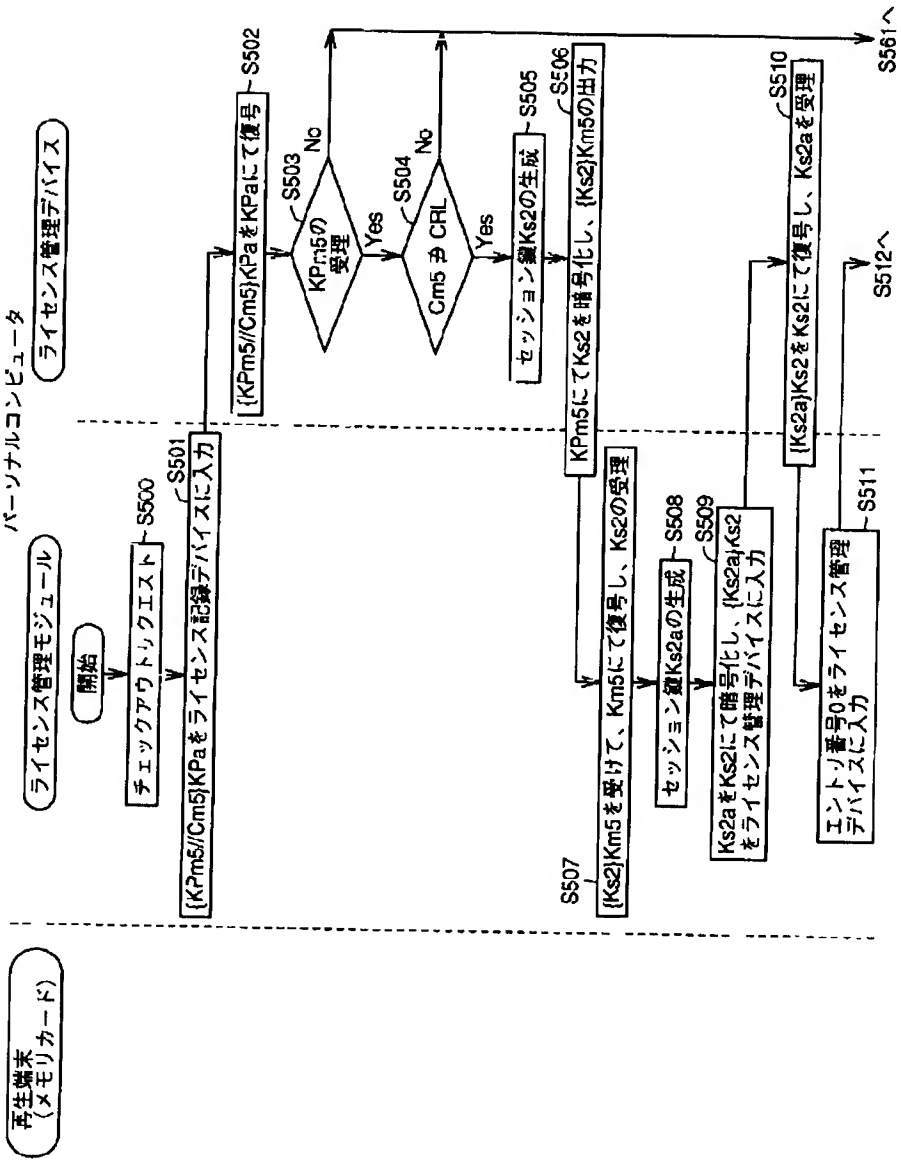
【図28】


再生装置
(メモリカード)
パーソナルコンピュータ
(ライセンス管理モジュール)
ライセンス管理デバイス
S346 or S348から
トランザクションID、コンテンツID、Kc、ACmおよびACpをKmc4にて暗号化し、
{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4を生成
S350
S352
CRL date
新しいか？
No
Yes
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4をKs2にて暗号化し、
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2の出力
S354
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2の送信
S356
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2の受信
S358
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2を{Kmc4}Ks2にて復号
S360
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4}Kmc4の受理
CRLをCRL領域より取得
S362
CRLと{{トランザクションID//コンテンツID//Kc//AC:m//ACp}Kmc4}をKs2にて暗号化し、
{CRL//{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2の出力
S364
{CRL//{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2の送信
S368
{CRL//{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2の受信
S370
{CRL//{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2を{Kmc4}Ks2にて復号
S372
{CRL//{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4}Kmc4の受理
CRLと{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc4}
S374
メモリ内のCRLを受理したCRLに書き換える
S376へ

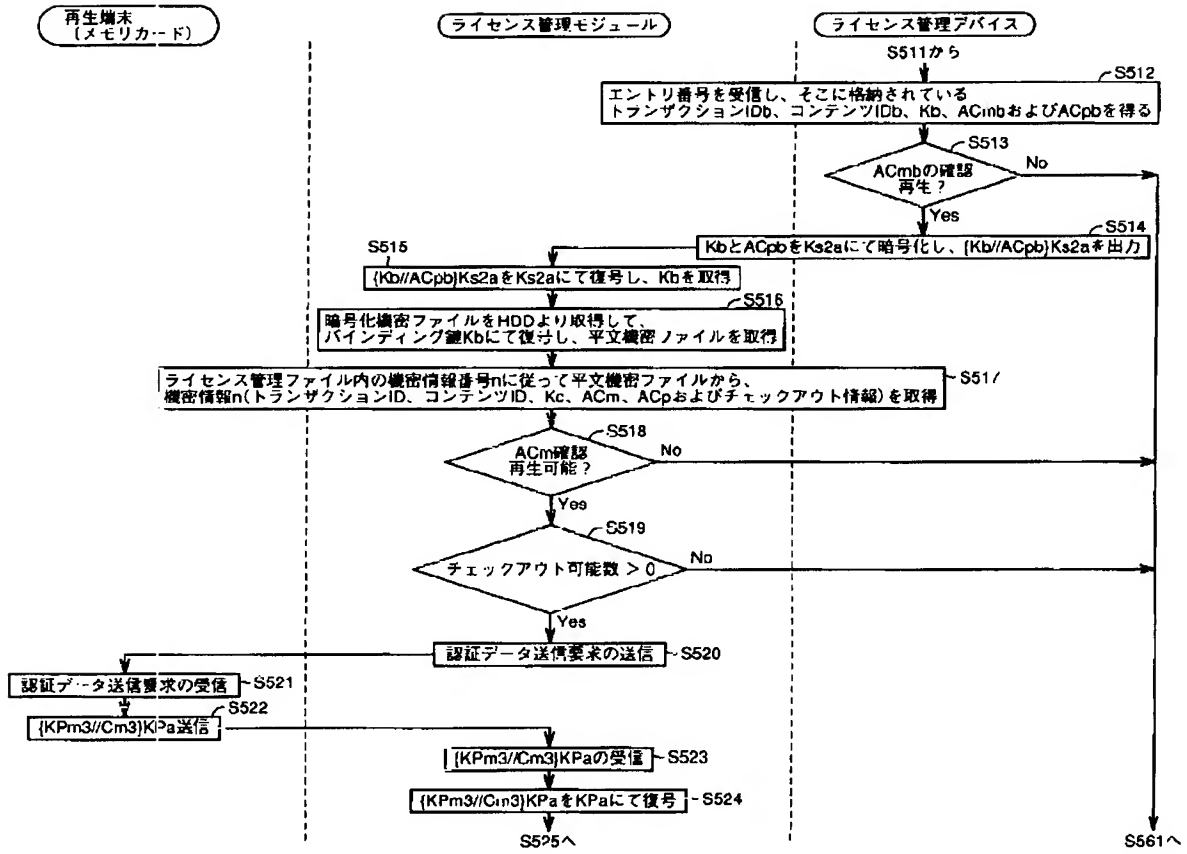
【図29】


再生端末
(メモリカード)
パーソナルコンピュータ
(ライセンス管理モジュール)
ライセンス管理デバイス
S360 or S374から
S312 or S314 or S346から
{トランザクションID//Kc//ACm//ACp}Kmc4をKmc4にて復号
トランザクションID、コンテンツID、Kc、ACmおよびACpの受理
S376
ライセンスを格納するためのエントリ番号を送信
S378
トランザクションID、コンテンツID、Kc、ACmおよびACpをライセンス領域の指示されたエントリに格納
S380
メモリカードのライセンスを格納したエントリ番号および平文のトランザクションIDおよびコンテンツIDを含むメモリカードへ移動しようとする{Dc}KcとDc-infに対するライセンス管理ファイルを生成し、メモリカードに送信
S382
複製？
S386
Yes
No
HDD内に記録された移動したライセンスに対するライセンス無に更新
S388
受信したライセンス管理ファイルをデータ領域に記録
S384
{Dc}KcとDc-infをHDDより取得し、{Dc}Kc//Dc-infを送信
S390
{Dc}Kc//Dc-infの受信
S392
{Dc}KcとDc-infをメモリのデータ領域に記録
S394
移動した楽曲を追記した再生リストを作成
S396
再生リストと書き換え指示を送信
S398
再生リストと書き換え指示を受信
S400
受信した再生リストに書き換え
S402
終了
S404

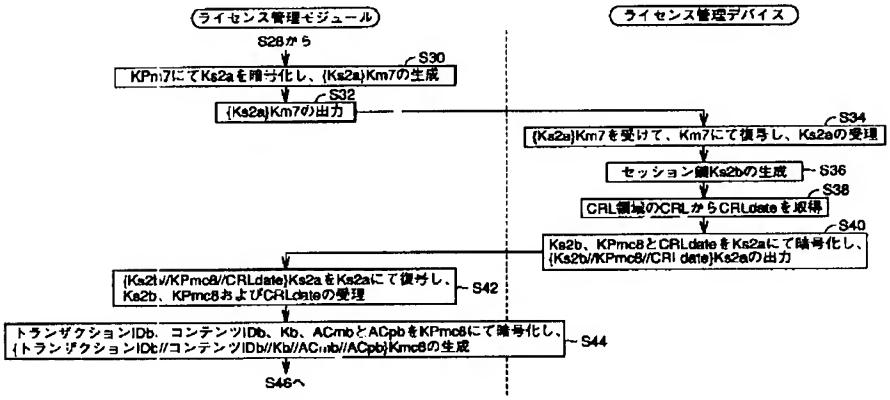
【図30】


再生端末
(メモリカード)
パーソナルコンピュータ
ライセンス管理モジュール
ライセンス管理デバイス
開始
チェックアウトリクエスト
S500
{KPm5//Cm5}KPaをライセンス記録デバイスに入力
S501
{KPm5//Cm5}KPaをKPaにて復号
S502
KPm5の受理
S503
No
Yes
Cm5 ≠ CRL
S504
No
Yes
セッション鍵Ks2の生成
S505
KPm5にてKs2を暗号化し、{Ks2}Km5の出力
S506
{Ks2}Km5を受けて、Km5にて復号し、Ks2の受理
S507
セッション鍵Ks2aの生成
S508
Ks2aをKs2にて暗号化し、{Ks2a}Ks2をライセンス管理デバイスに入力
S509
{Ks2a}Ks2をKs2にて復号し、Ks2aを受理
S510
エントリ番号0をライセンス管理デバイスに入力
S511
S512へ
S561へ

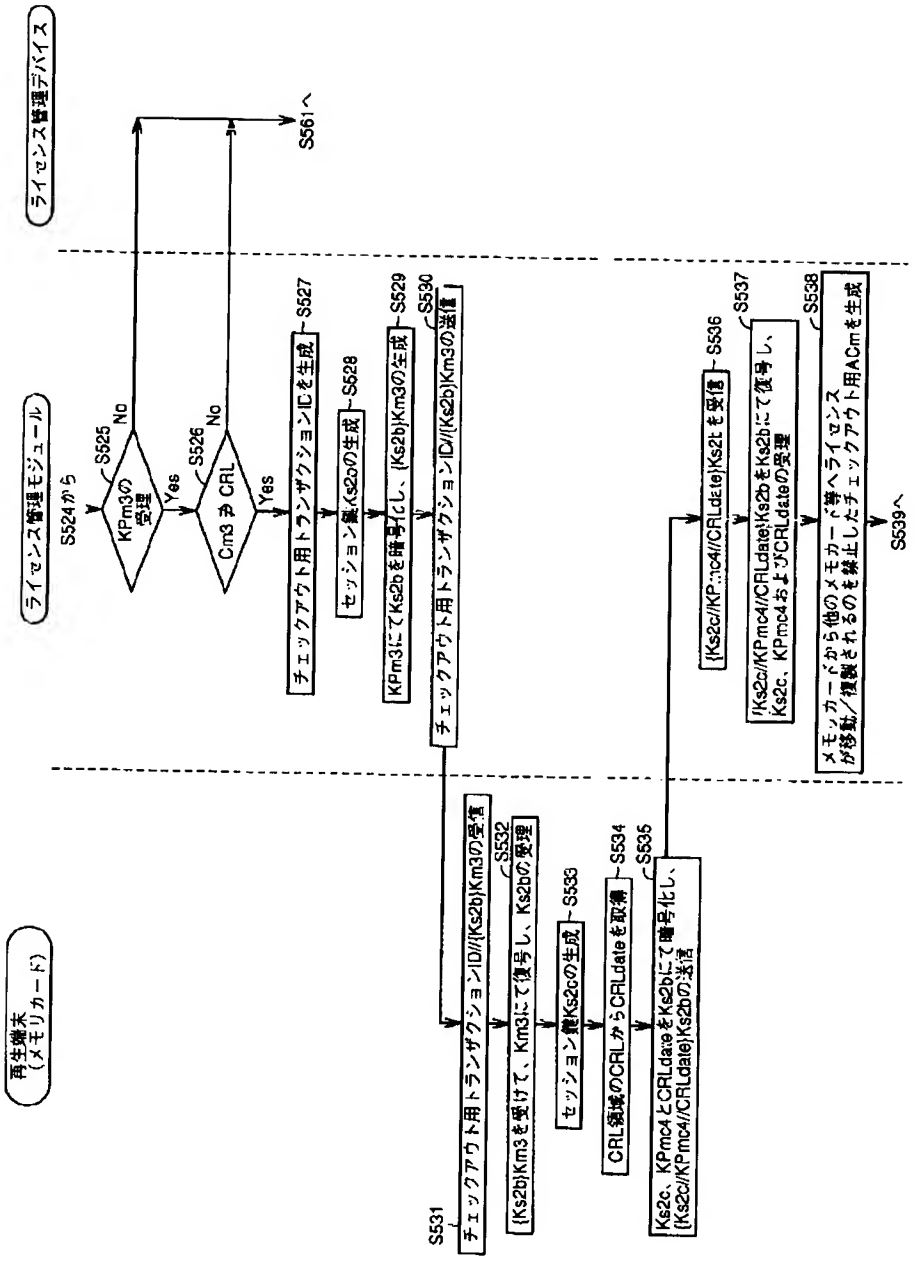
【図31】


再生端末
(メモリカード)
ライセンス管理モジュール
ライセンス管理デバイス
S511から
S512
エントリ番号を受信し、そこに格納されている
トランザクションIDb、コンテンツIDb、Kb、ACmbおよびACpbを得る
S513
ACmbの確認
再生？
No
Yes
S514
KbとACpbをKs2aにて暗号化し、{Kb//ACpb}Ks2aを出力
S515
{Kb//ACpb}Ks2aをKs2aにて復号し、Kbを取得
S516
暗号化機密ファイルをHDDより取得して、
バインディング鍵Kbにて復号し、平文機密ファイルを取得
ライセンス管理ファイル内の機密情報番号nに従って平文機密ファイルから、
機密情報n(トランザクションID、コンテンツID、Kc、ACm、ACpおよびチェックアウト情報)を取得
S517
S518
ACm確認
再生可能？
No
Yes
S519
チェックアウト可能数＞0
No
Yes
認証データ送信要求の送信
S520
認証データ送信要求の受信
S521
S522
{KPm3//Cm3}KPa送信
{KPm3//Cm3}KPaの受信
S523
{KPm3//Cm3}KPaをKPaにて復号
S524
S525へ
S561へ

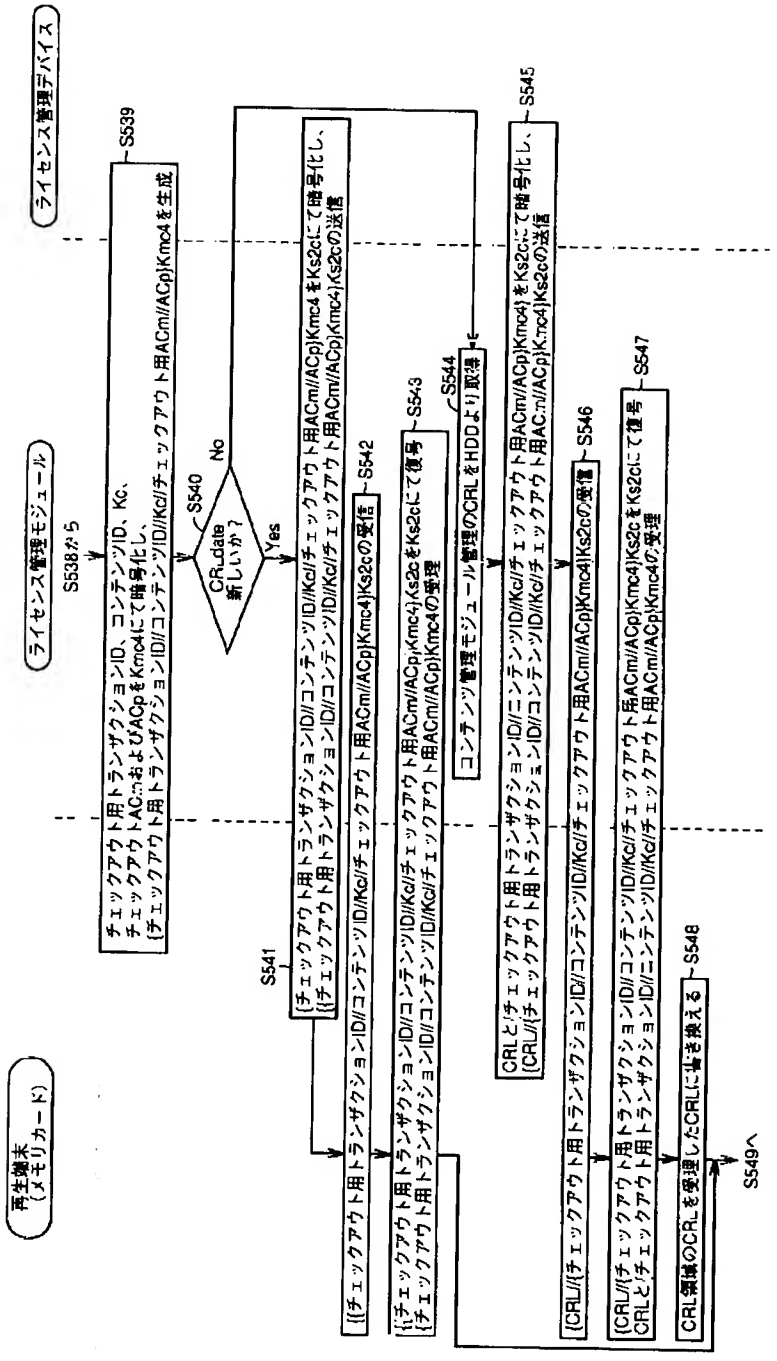
【図51】


ライセンス管理モジュール
ライセンス管理デバイス
S28から
S30
KPm7にてKs2aを暗号化し、{Ks2a}Km7の生成
S32
{Ks2a}Km7の出力
S34
{Ks2a}Km7を受けて、Km7にて復号し、Ks2aの受理
セッション鍵Ks2bの生成
S36
S38
CRL領域のCRLからCRLdateを取得
S40
Ks2b、KPmc8とCRLdateをKs2aにて暗号化し、
{Ks2b//KPmc8//CRLdate}Ks2aの出力
{Ks2b//KPmc8//CRLdate}Ks2aをKs2aにて復号し、
Ks2b、KPmc8およびCRLdateの受理
S42
トランザクションIDb、コンテンツIDb、Kb、ACmbとACpbをKPmc8にて暗号化し、
{トランザクションIDb//コンテンツIDb//Kb//ACmb//ACpb}Kmc8の生成
S44
S46へ

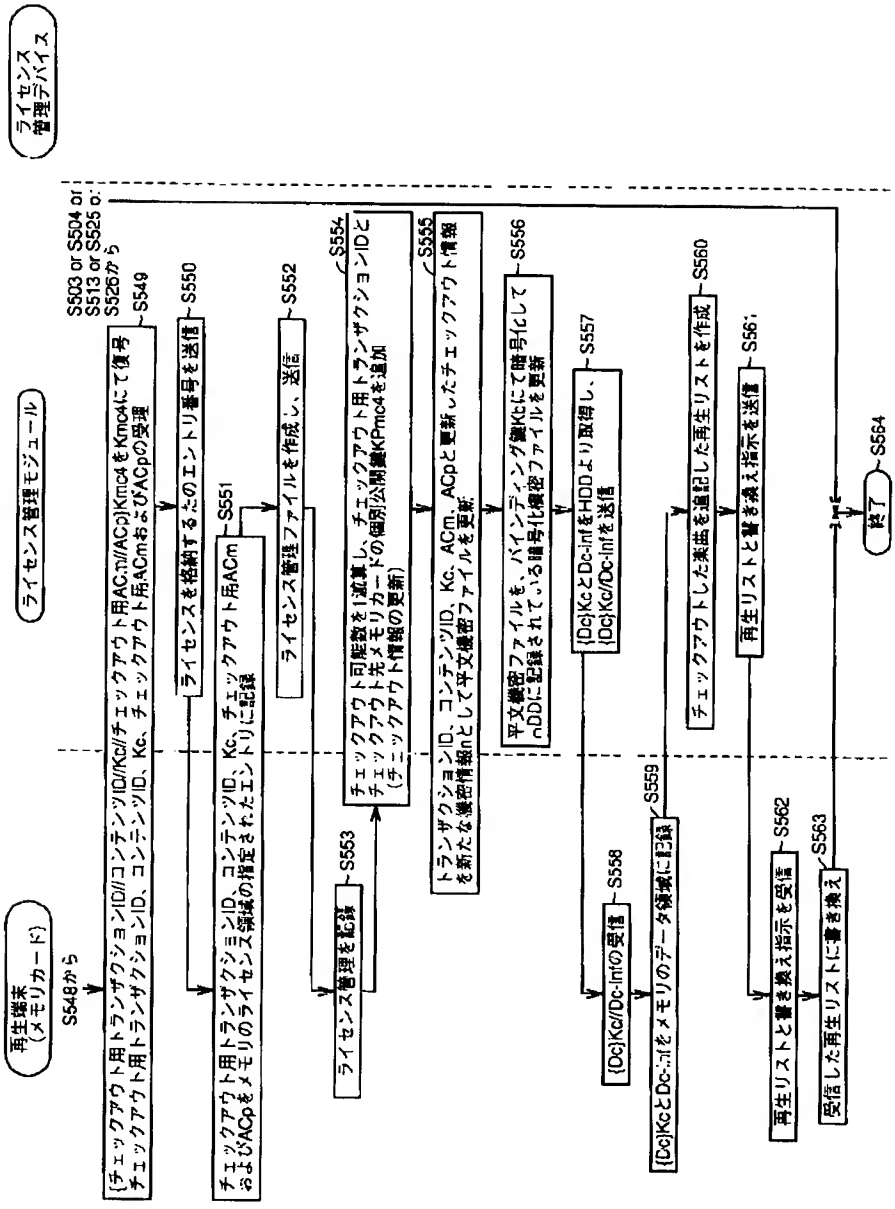
【図32】


再生端末
(メモリカード)
ライセンス管理モジュール
ライセンス管理デバイス
S524から
S525
KPm3の受理
No
Yes
S526
Cm3 ⇒ CRL
No
Yes
S561へ
チェックアウト用トランザクションIDを生成
S527
セッション鍵Ks2cの生成
S528
KPm3にてKs2bを暗号化し、{Ks2b}Km3の生成
S529
チェックアウト用トランザクションID//{Ks2b}Km3の送信
S530
S531
チェックアウト用トランザクションID//{Ks2b}Km3の受信
S532
{Ks2b}Km3を受けて、Km3にて復号し、Ks2bの受理
S533
セッション鍵Ks2cの生成
S534
CRL登録のCRLからCRLdateを取得
S535
Ks2c、KPmc4とCRLdateをKs2bにて暗号化し、
{Ks2c//KPmc4//CRLdate}Ks2bの送信
{Ks2c//KPmc4//CRLdate}Ks2bを受信
S536
{Ks2c//KPmc4//CRLdate}Ks2bをKs2bにて復号し、
Ks2c、KPmc4およびCRLdateの受理
S537
メモリカードから他のメモカード等へライセンス
が移動／複製されるのを禁止したチェックアウト用ACmを生成
S538
S539へ

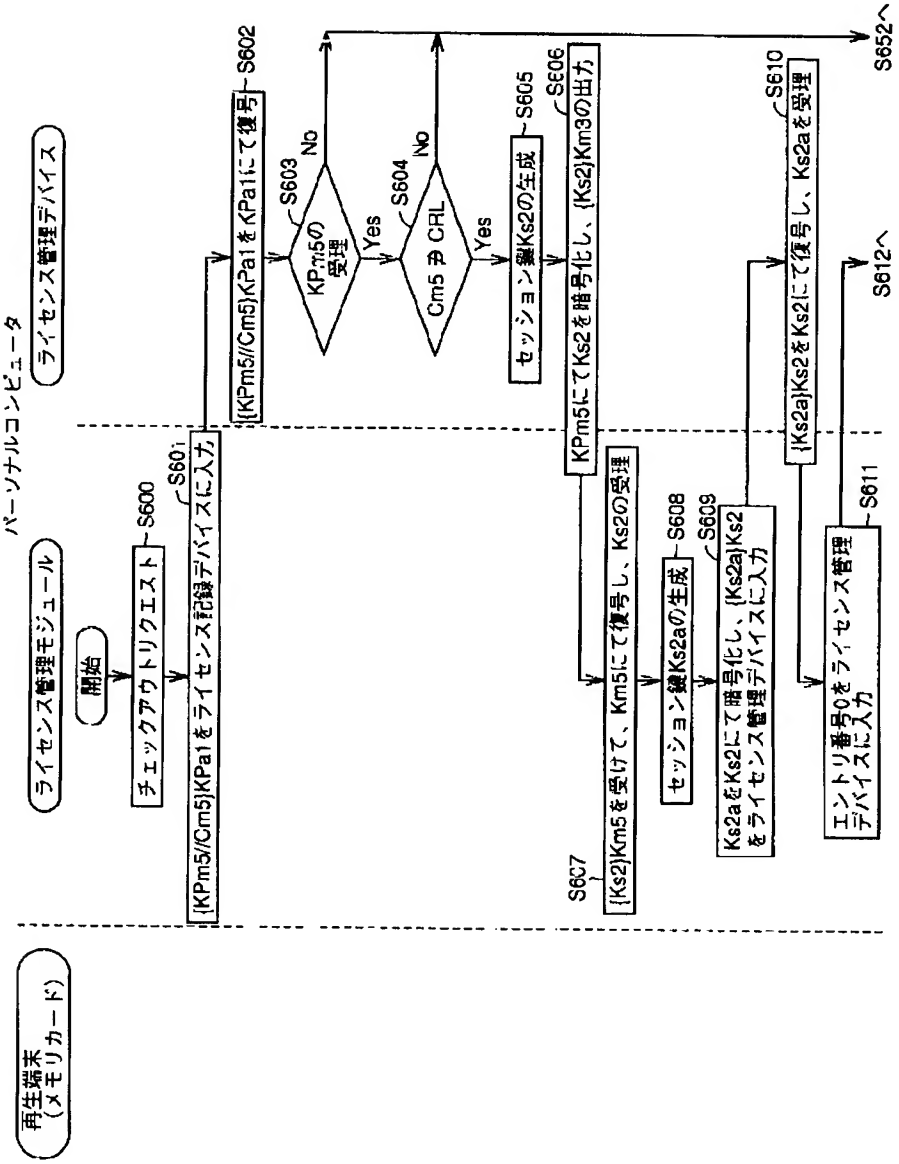
【図33】


再生端末
(メモリカード)
ライセンス管理モジュール
ライセンス管理デバイス
S538から
チェックアウト用トランザクションID、コンテンツID、Kc、
チェックアウトACmおよびACpをKmc4にて暗号化し、
{チェックアウト用トランザクションID//Kc//チェックアウト用ACm//ACp}Kmc4を生成
S539
S540
CRLdate
新しいか？
No
Yes
S541
{チェックアウト用トランザクションID//コンテンツID//Kc//チェックアウト用ACm//ACp}Kmc4をKs2cにて暗号化し、
{{チェックアウト用トランザクションID//コンテンツID//Kc//チェックアウト用ACm//ACp}Kmc4}Ks2cの送信
{{チェックアウト用トランザクションID//コンテンツID//Kc//チェックアウト用ACm//ACp}Kmc4}Ks2cの受信
S542
{{チェックアウト用トランザクションID//コンテンツID//Kc//チェックアウト用ACm//ACp}Kmc4}Ks2cをKs2cにて復号
S543
{{チェックアウト用トランザクションID//コンテンツID//Kc//チェックアウト用ACm//ACp}Kmc4の受理
S544
コンテンツ管理モジュール管理のCRLをHDDより取得
CRLと{{チェックアウト用トランザクションID//コンテンツID//Kc//チェックアウト用ACm//ACp}Kmc4}をKs2cにて暗号化し、
{CRL//{チェックアウト用トランザクションID//コンテンツID//Kc//チェックアウト用ACm//ACp}Kmc4}Ks2cの送信
S545
{CRL//{チェックアウト用トランザクションID//コンテンツID//Kc//チェックアウト用ACm//ACp}Kmc4}Ks2cの受信
S546
{CRL//{チェックアウト用トランザクションID//コンテンツID//Kc//チェックアウト用ACm//ACp}Kmc4}Ks2cをKs2cにて復号
CRLと{チェックアウト用トランザクションID//コンテンツID//Kc//チェックアウト用ACm//ACp}Kmc4の受理
S547
CRL領域のCRLを受理したCRLに書き換える
S548
S549へ

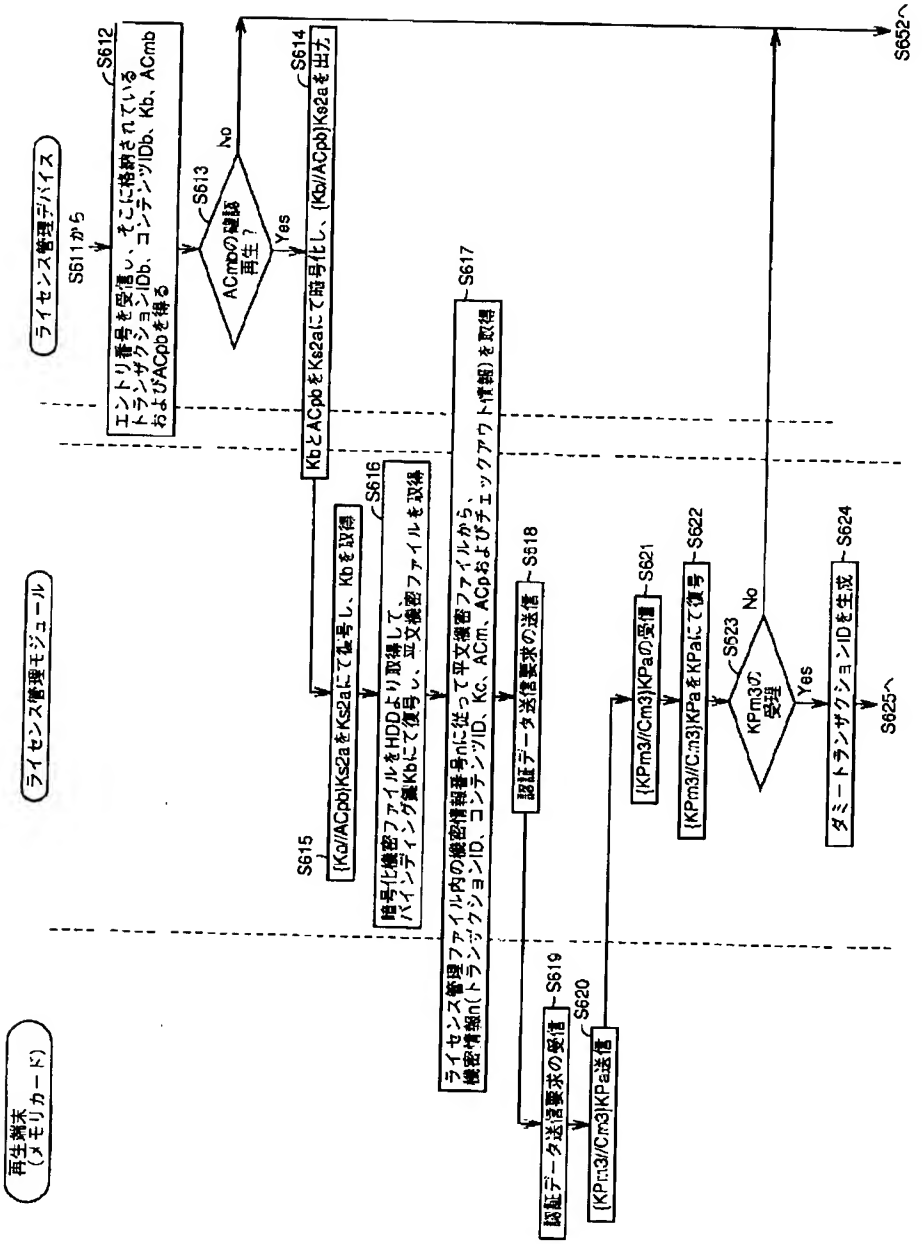
【図34】


再生端末
(メモリカード)
ライセンス管理モジュール
ライセンス
管理デバイス
S548から
{チェックアウト用トランザクションID//コンテンツID//Kc//チェックアウト用ACm//ACp}Kmc4をKmc4にて復号
チェックアウト用トランザクションID、コンテンツID、Kc、チェックアウト用ACmおよびACpの受理
S549
S503 or S504 or S525 or S526から
ライセンスを格納するためのエントリ番号を送信
S550
チェックアウト用トランザクションID、コンテンツID、Kc、チェックアウト用ACm
およびACpをメモリのライセンス領域の指定されたエントリに記録
S551
ライセンス管理ファイルを作成し、送信
S552
ライセンス管理を記録
S553
チェックアウト可能数を1減算し、チェックアウト用トランザクションIDと
チェックアウト先メモリカードの個別公開鍵KPmc4を追加
(チェックアウト情報の更新)
S554
トランザクションID、コンテンツID、Kc、ACm、ACpと更新したチェックアウト情報
を新たな機密情報nとして平文機密ファイルを更新
S555
平文機密ファイルを、バインディング鍵Kcにて暗号化して
nDDに記録されている暗号化機密ファイルを更新
S556
{Dc}Kc/{Dc-Inf}の受信
S558
{Dc}KcとDc-InfをHDDより取得し、
{Dc}Kc//Dc-Inf}を送信
S557
{Dc}KcとDc-Inf}をメモリのデータ領域に記録
S559
チェックアウトした楽曲を追記した再生リストを作成
S560
再生リストと書き換え指示を送信
S561
再生リストと書き換え指示を受信
S562
受信した再生リストに書き換え
S563
終了
S564

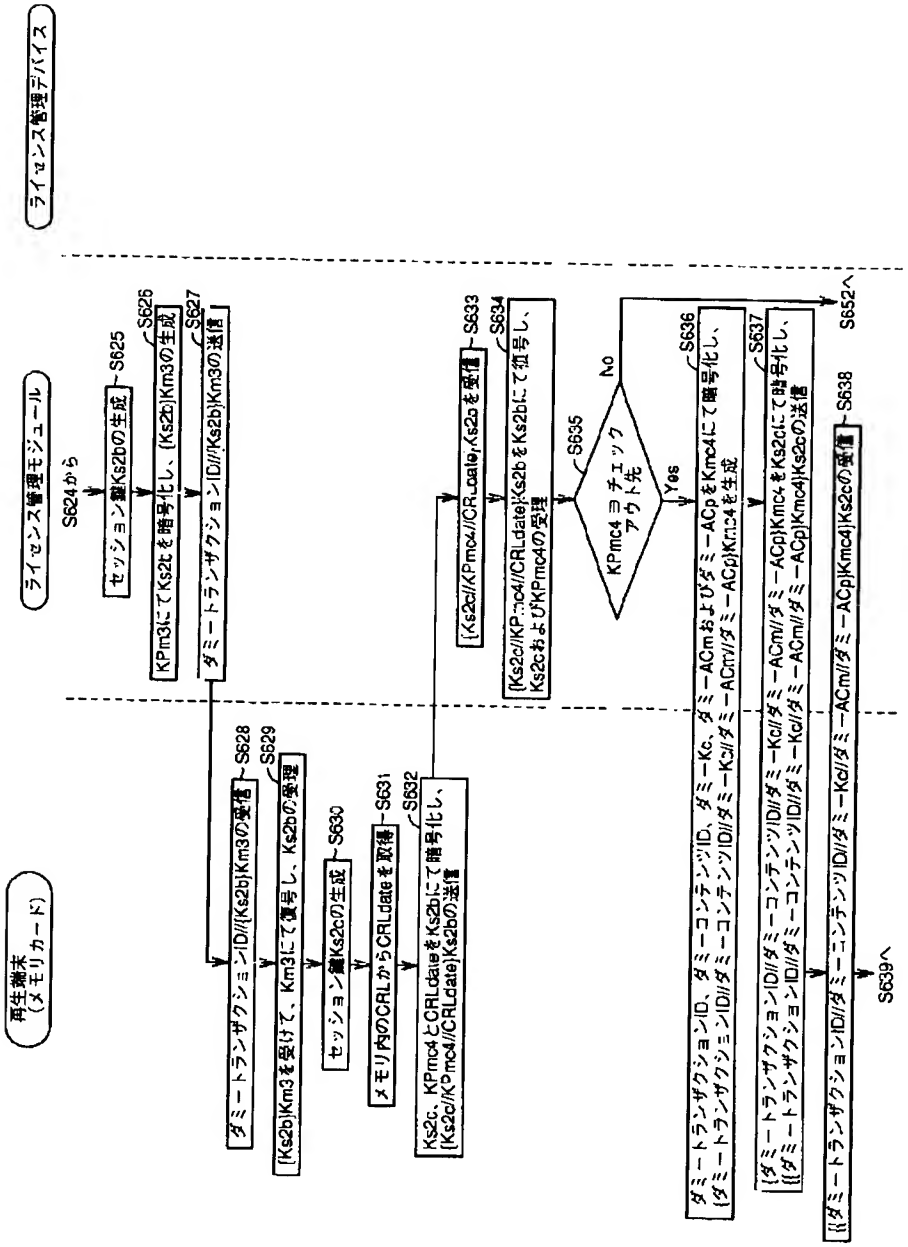
【図35】


再生端末
(メモリカード)
パーソナルコンピュータ
ライセンス管理モジュール
ライセンス管理デバイス
開始
チェックアウトリクエスト
S600
{KPm5//Cm5}KPa1をライセンス記録デバイスに入力
S601
{KPm5//Cm5}KPa1をKPa1にて復号
S602
KPm5の受理
S603
No
Yes
Cm5 ≠ CRL
S604
No
Yes
セッション鍵Ks2の生成
S605
KPm5にてKs2を暗号化し、{Ks2}Km3の出力
S606
{Ks2}Km5を受けて、Km5にて復号し、Ks2の受理
S607
セッション鍵Ks2aの生成
S608
Ks2aをKs2にて暗号化し、{Ks2a}Ks2をライセンス管理デバイスに入力
S609
{Ks2a}Ks2をKs2にて復号し、Ks2aを受理
S610
エントリ番号0をライセンス管理デバイスに入力
S611
S612へ
S652へ

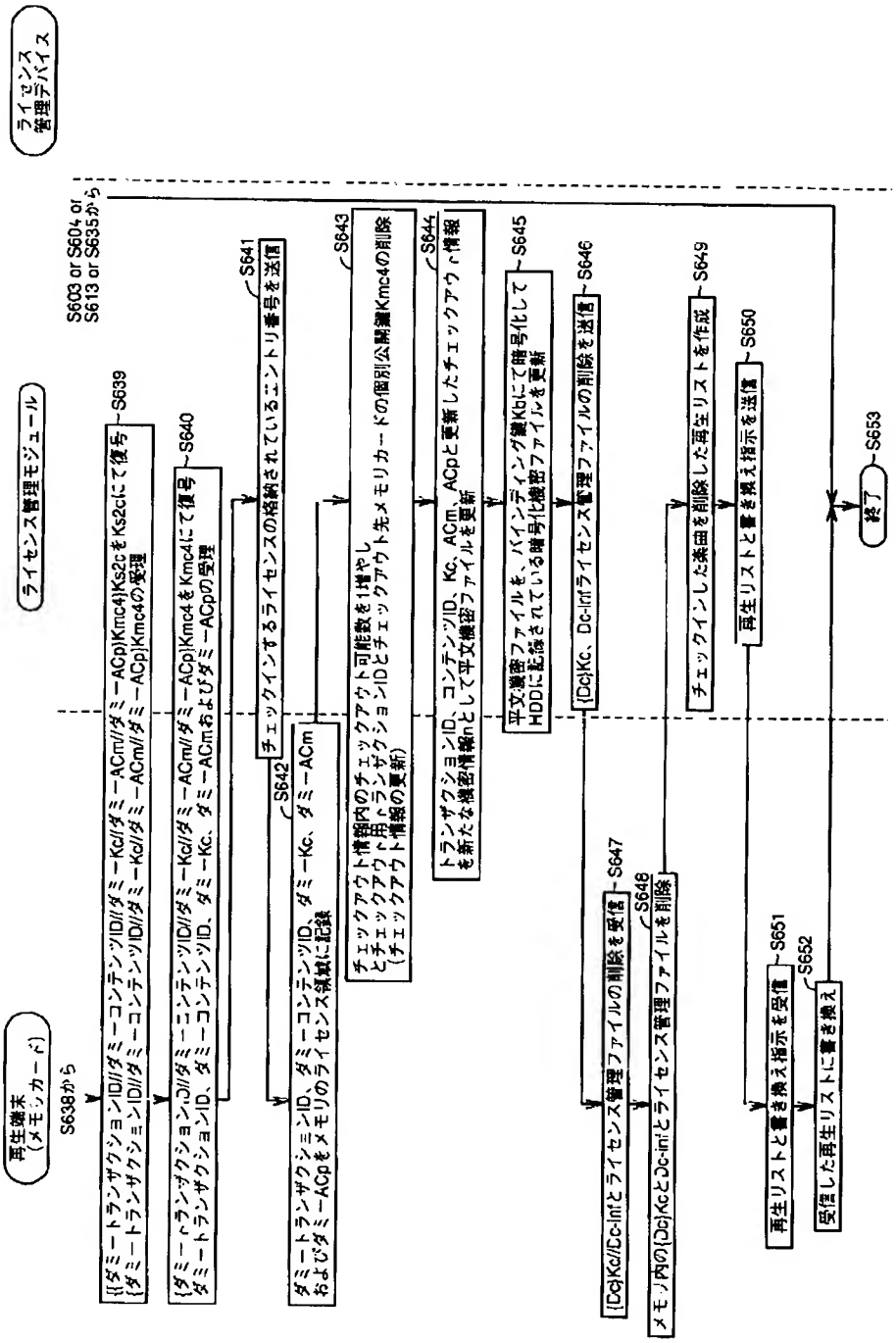
【図36】


再生端末
(メモリカード)
ライセンス管理モジュール
ライセンス管理デバイス
S611から
S612
エントリ番号を受信し、そこに格納されている
トランザクションIDb、コンテンツIDb、Kb、ACmb
およびACpbを得る
S613
ACmbの鍵
再生?
No
Yes
S614
KbとACpbをKs2aにて暗号化し、{Kb//ACpb}Ks2aを出力
S615
{Kb//ACpb}Ks2aをKs2aにて復号し、Kbを取得
S616
暗号化機密ファイルをHDDより取得して、
バインディング鍵Kbにて復号し、平文機密ファイルを取得
S617
ライセンス管理ファイル内の機密情報番号nに従って平文機密ファイルから、
機密情報n(トランザクションID、Kc、ACm、ACpおよびチェックアウト情報)を取得
S618
認証データ送信要求の送信
S619
認証データ送信要求の受信
S620
{KPm3//Cm3}KPa送信
S621
{KPm3//Cm3}KPaの受信
S622
{KPm3//Cm3}KPaをKPaにて復号
S623
KPm3の
受理
No
Yes
S624
ダミートランザクションIDを生成
S625へ
S652へ

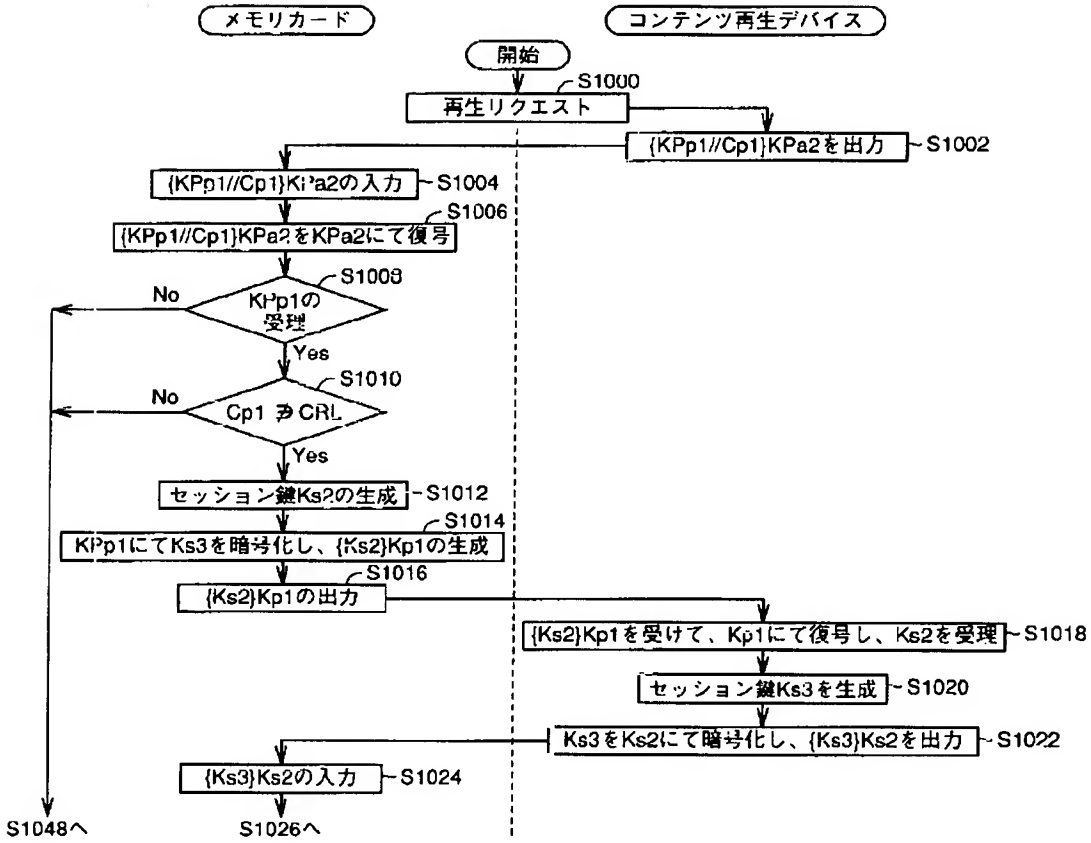
【図37】


再生端末
(メモリカード)
ライセンス管理モジュール
ライセンス管理デバイス
S624から
セッション鍵Ks2bの生成
S625
KPm3にてKs2cを暗号化し、(Ks2b)Km3の生成
S626
ダミートランザクションID//(Ks2b)Km3の送信
S627
ダミートランザクションID//(Ks2b)Km3の受信
S628
(Ks2b)Km3を受けて、Km3にて復号し、Ks2bの取得
S629
セッション鍵Ks2cの生成
S630
メモリ内のCRLからCRLdateを取得
S631
Ks2c、KPmc4とCRLdateをKs2bにて暗号化し、
(Ks2c//KPmc4//CRLdate)Ks2bの送信
S632
(Ks2c//KPmc4//CRLdate)Ks2bの受信
S633
(Ks2c//KPmc4//CRLdate)Ks2bをKs2bにて復号し、
Ks2cおよびKPmc4の取得
S634
KPmc4 ヨチェック アウト先
S635
No
Yes
ダミートランザクションID、ダミーコンテンツID、ダミーKc、ダミーACmおよびダミーACpをKmc4にて暗号化し、
(ダミートランザクションID//ダミーコンテンツID//ダミーKc//ダミーACm//ダミーACp)Kmc4を生成
S636
(ダミートランザクションID//ダミーコンテンツID//ダミーKc//ダミーACm//ダミーACp)Kmc4をKs2cにて暗号化し、
((ダミートランザクションID//ダミーコンテンツID//ダミーKc//ダミーACm//ダミーACp)Kmc4)Ks2cの送信
S637
((ダミートランザクションID//ダミーコンテンツID//ダミーKc//ダミーACm//ダミーACp)Kmc4)Ks2cの受信
S638
S639へ
S652へ

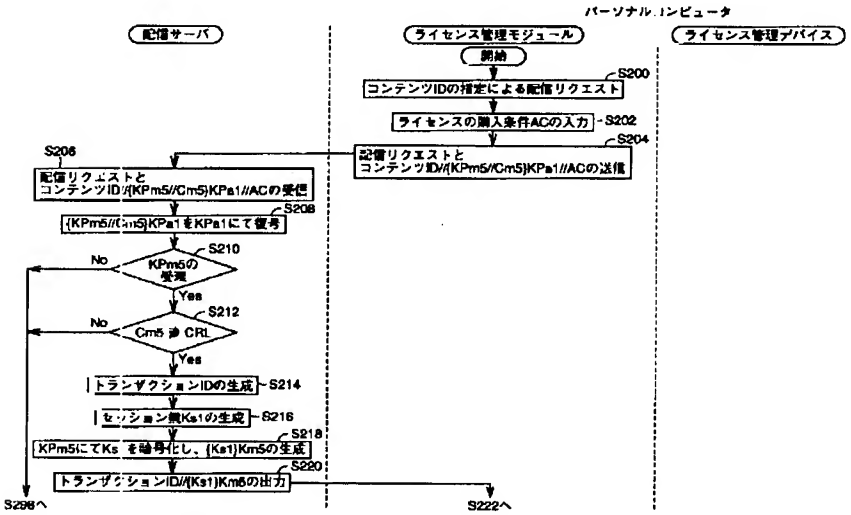
【図38】


再生端末
(メモリカード)
ライセンス
管理デバイス
ライセンス管理モジュール
S638から
S603 or S604 or
S613 or S635から
{{ダミーKc//ダミーACm//ダミーACp}Kmc4}Ks2cをKs2cにて復号
{ダミートランザクションID//ダミーコンテンツID//ダミーKc//ダミーACm//ダミーACp}Kmc4の受理
{ダミートランザクションID//ダミーコンテンツID//ダミーKc//ダミーACm//ダミーACp}Kmc4をKmc4にて復号
ダミートランザクションID、ダミーコンテンツID、ダミーKc、ダミーACmおよびダミーACpの受理
チェックインするライセンスの格納されているエントリ番号を送信
ダミートランザクションID、ダミーコンテンツID、ダミーKc、ダミーACm
およびダミーACpをメモリのライセンス様式に記録
チェックアウト情報内のチェックアウト可能数を1増やし
とチェックアウト用トランザクションIDとチェックアウト先メモリカードの個別公開鍵Kmc4の削除
(チェックアウト情報の更新)
トランザクションID、コンテンツID、Kc、ACm、ACpと更新したチェックアウト情報
を新たな機密情報nとして平文機密ファイルを更新
平文機密ファイルを、バインディング鍵Kbにて暗号化して
HDDに転送されている暗号化機密ファイルを更新
{Dc}Kc、Dc-infライセンス管理ファイルの削除を送信
{Dc}Kc//Dc-infとライセンス管理ファイルの削除を受信
メモリ内の{Dc}KcとDc-infとライセンス管理ファイルを削除
チェックインした楽曲を削除した再生リストを作成
再生リストと書き換え指示を送信
再生リストと書き換え指示を受信
受信した再生リストに書き換え
終了
S639
S640
S641
S642
S643
S644
S645
S646
S647
S648
S649
S650
S651
S652
S653

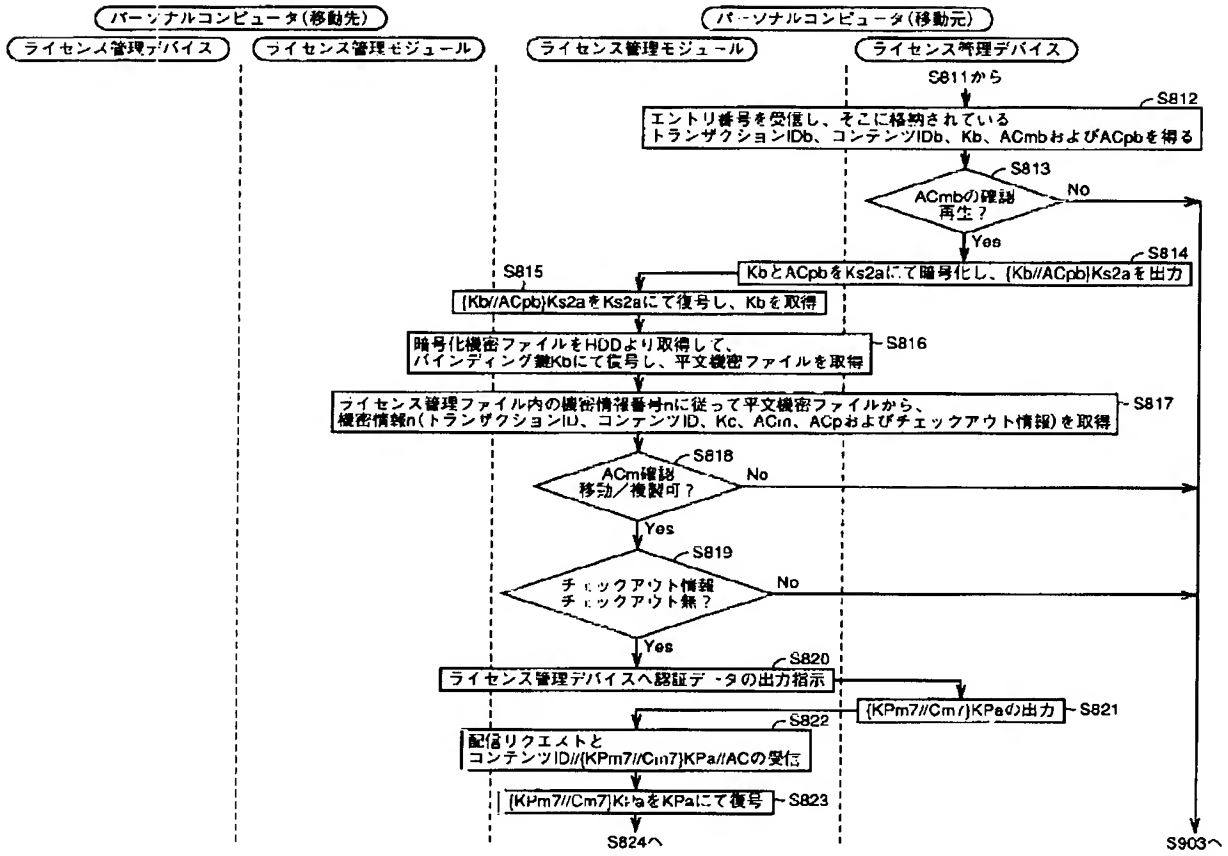
【図39】


メモリカード
コンテンツ再生デバイス
開始
S1000
再生リクエスト
{KPp1//Cp1}KPa2を出力
S1002
{KPp1//Cp1}KPa2の入力
S1004
S1006
{KPp1//Cp1}KPa2をKPa2にて復号
S1008
No
KPp1の受理
Yes
S1010
No
Cp1 ≠ CRL
Yes
セッション鍵Ks2の生成
S1012
S1014
KPp1にてKs3を暗号化し、{Ks2}Kp1の生成
S1016
{Ks2}Kp1の出力
{Ks2}Kp1を受けて、Kp1にて復号し、Ks2を受理
S1018
セッション鍵Ks3を生成
S1020
Ks3をKs2にて暗号化し、{Ks3}Ks2を出力
S1022
{Ks3}Ks2の入力
S1024
S1048へ
S1026へ

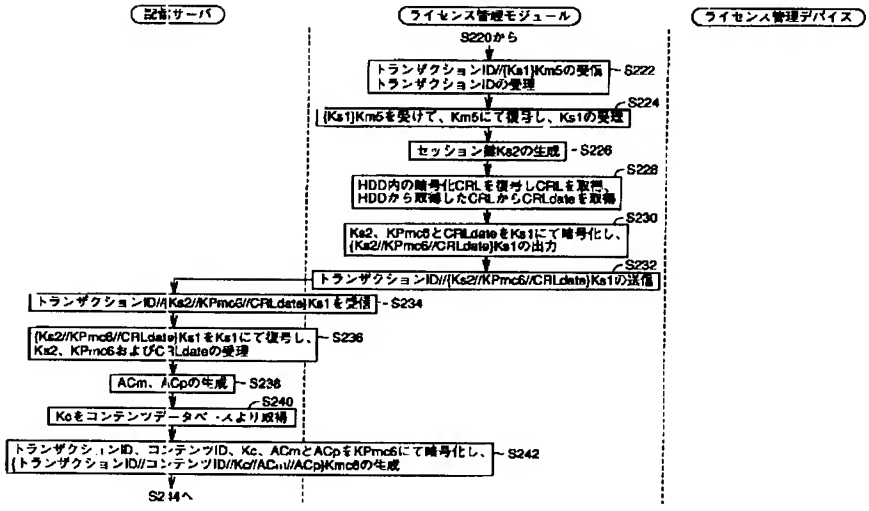
【図53】


パーソナルコンピュータ
配信サーバ
ライセンス管理モジュール
ライセンス管理デバイス
開始
S200
コンテンツIDの指定による配信リクエスト
ライセンスの購入条件ACの入力
S202
S204
配信リクエストと
コンテンツID/{KPm5/Cm5}KPa1//ACの送信
S206
配信リクエストと
コンテンツID/{KPm5/Cm5}KPa1//ACの受信
S208
{KPm5//Cm5}KPa1をKPa1にて復号
S210
No
KPm5の受理
Yes
S212
No
Cm5 ≠ CRL
Yes
トランザクションIDの生成
S214
セッション鍵Ks1の生成
S216
S218
KPm5にてKs1を暗号化し、{Ks1}Km5の生成
S220
トランザクションID/{Ks1}Km5の出力
S296へ
S222へ

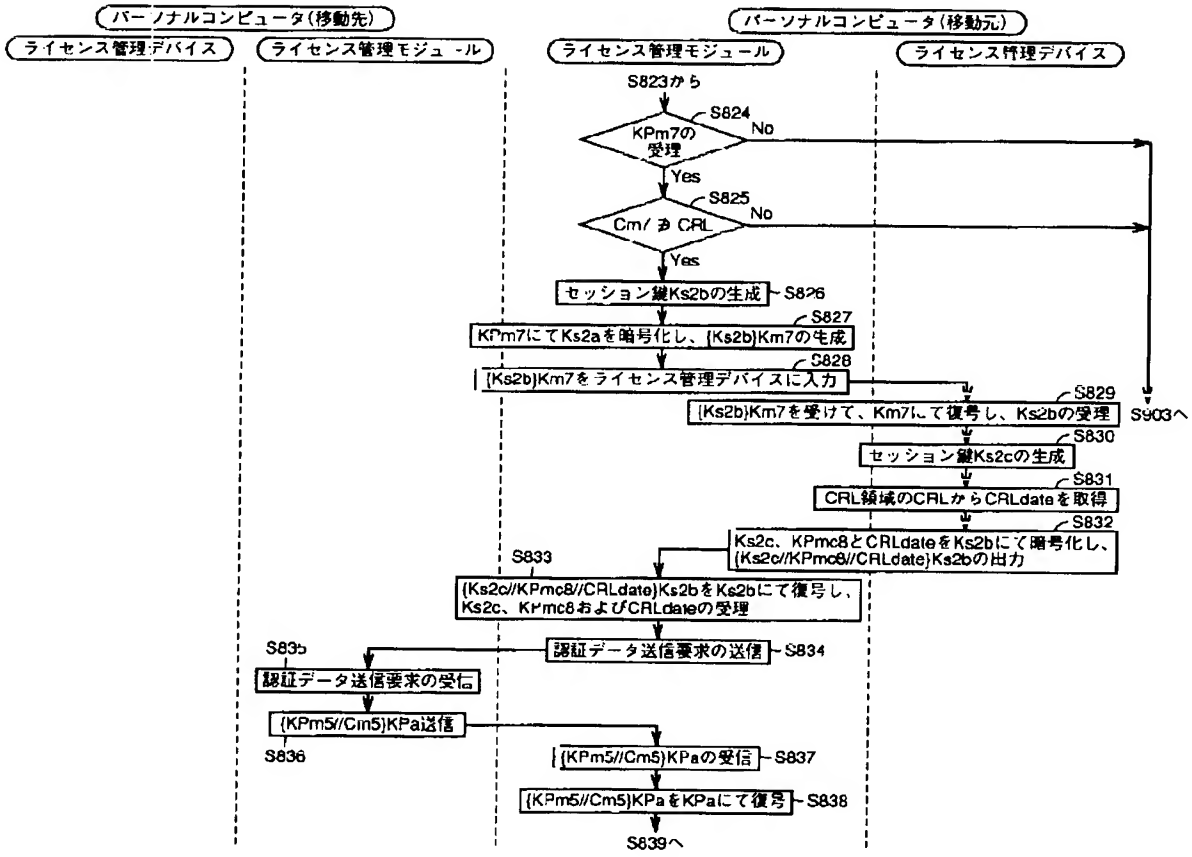
【図42】


パーソナルコンピュータ(移動先)
ライセンス管理デバイス
ライセンス管理モジュール
パーソナルコンピュータ(移動元)
ライセンス管理モジュール
ライセンス管理デバイス
S811から
S812
エントリ番号を受信し、そこに格納されている
トランザクションIDb、コンテンツIDb、Kb、ACmbおよびACpbを得る
S813
ACmbの確認
再生？
No
Yes
S814
KbとACpbをKs2aにて暗号化し、{Kb//ACpb}Ks2aを出力
S815
{Kb//ACpb}Ks2aをKs2aにて復号し、Kbを取得
暗号化機密ファイルをHDDより取得して、
バインディング鍵Kbにて復号し、平文機密ファイルを取得
S816
ライセンス管理ファイル内の機密情報番号nに従って平文機密ファイルから、
機密情報n(トランザクションID、コンテンツID、Kc、ACm、ACpおよびチェックアウト情報)を取得
S817
S818
ACm確認
移動／複製可？
No
Yes
S819
チェックアウト情報
チェックアウト無？
No
Yes
S820
ライセンス管理デバイスへ認証データの出力指示
{KPm7//Cm7}KPaの出力
S821
S822
配信リクエストと
コンテンツID//{KPm7//Cm7}KPa//ACの受信
{KPm7//Cm7}KPaをKPaにて復号
S823
S824へ
S903へ

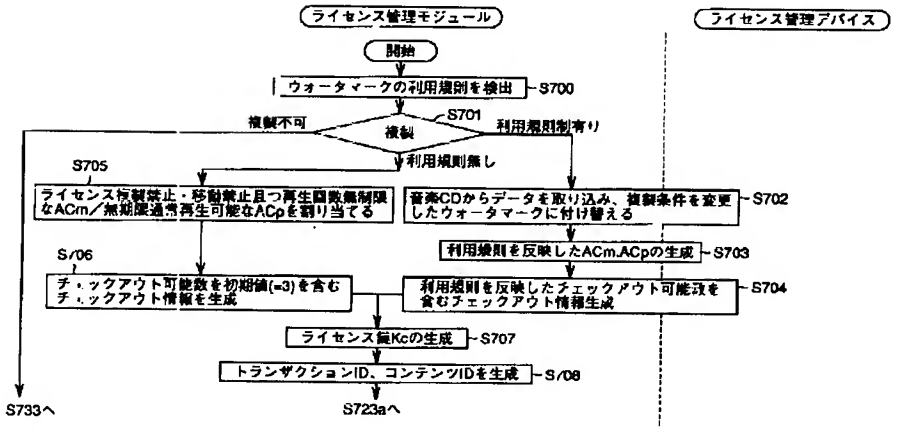
【図54】


配信サーバ
ライセンス管理モジュール
ライセンス管理デバイス
S220から
トランザクションID//{Ks1}Km5の受信
トランザクションIDの受理
S222
{Ks1}Km5を受けて、Km5にて復号し、Ks1の受理
S224
セッション鍵Ks2の生成
S226
HDD内の暗号化CRLを復号しCRLを取得、
HDDから取得したCRLからCRLdateを取得
S228
Ks2、KPmc6とCRLdateをKs1にて暗号化し、
{Ks2//KPmc6//CRLdate}Ks1の出力
S230
トランザクションID//{Ks2//KPmc6//CRLdate}Ks1の送信
S232
トランザクションID//{Ks2//KPmc6//CRLdate}Ks1を受信
S234
{Ks2//KPmc6//CRLdate}Ks1をKs1にて復号し、
Ks2、KPmc6およびCRLdateの受理
S236
ACm、ACpの生成
S238
Kcをコンテンツデータベースより取得
S240
トランザクションID、コンテンツID、Kc、ACmとACpをKPmc6にて暗号化し、
{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc6の生成
S242
S214へ

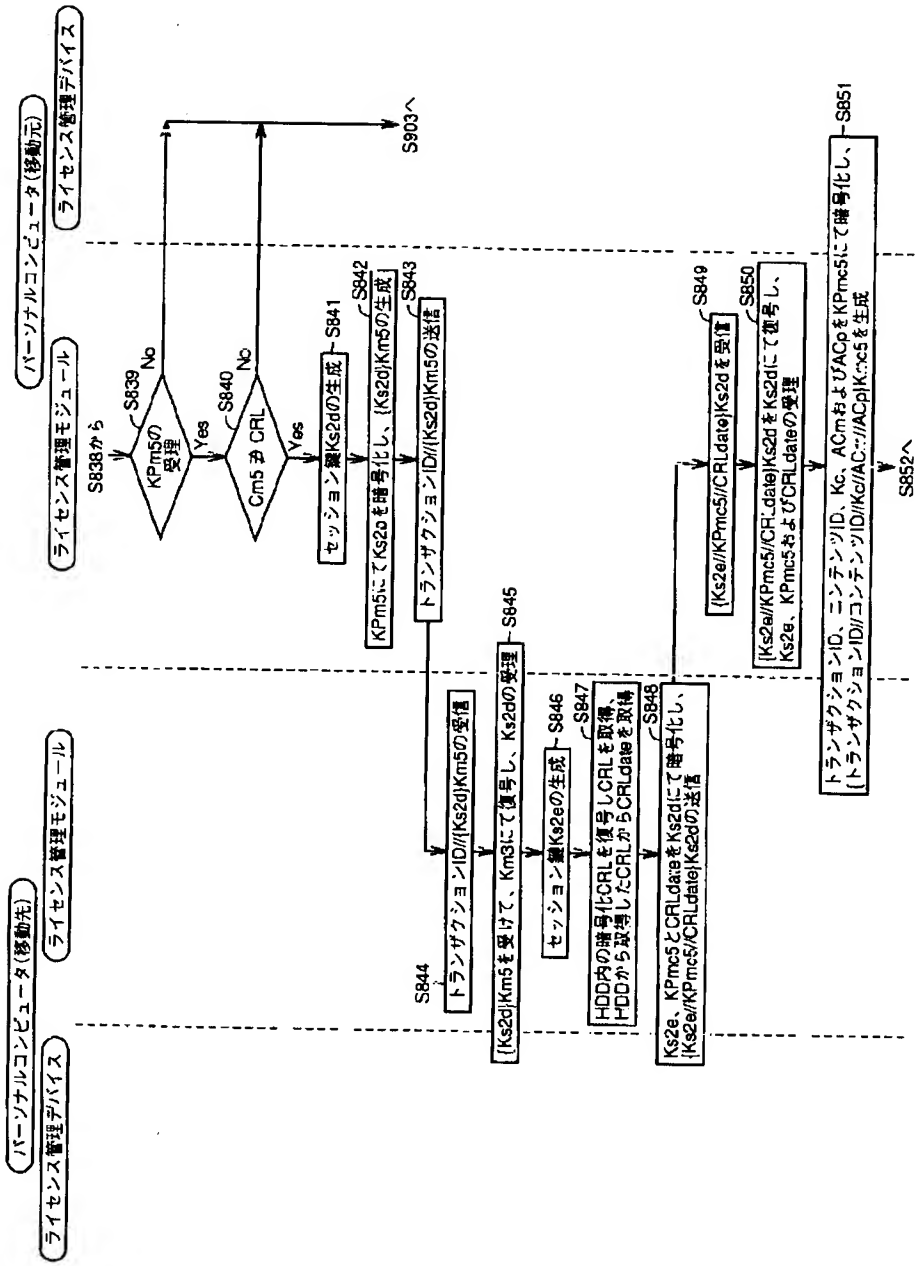
【図43】


パーソナルコンピュータ(移動先)
ライセンス管理デバイス
ライセンス管理モジュール
パーソナルコンピュータ(移動元)
ライセンス管理モジュール
ライセンス管理デバイス
S823から
S824
KPm7の受理
No
Yes
S825
Cm/あCRL
No
Yes
セッション鍵Ks2bの生成
S826
S827
KPm7にてKs2aを暗号化し、{Ks2b}Km7の生成
S828
{Ks2b}Km7をライセンス管理デバイスに入力
S829
{Ks2b}Km7を受けて、Km7にて復号し、Ks2bの受理
S903へ
S830
セッション鍵Ks2cの生成
S831
CRL領域のCRLからCRLdateを取得
S832
Ks2c、KPmc8とCRLdateをKs2bにて暗号化し、{Ks2c//KPmc8//CRLdate}Ks2bの出力
S833
{Ks2c//KPmc8//CRLdate}Ks2bをKs2bにて復号し、Ks2c、KPmc8およびCRLdateの受理
S835
認証データ送信要求の送信
S834
認証データ送信要求の受信
{KPm5//Cm5}KPai送信
S836
{KPm5//Cm5}KPaの受信
S837
{KPm5//Cm5}KPaをKPaにて復号
S838
S839へ

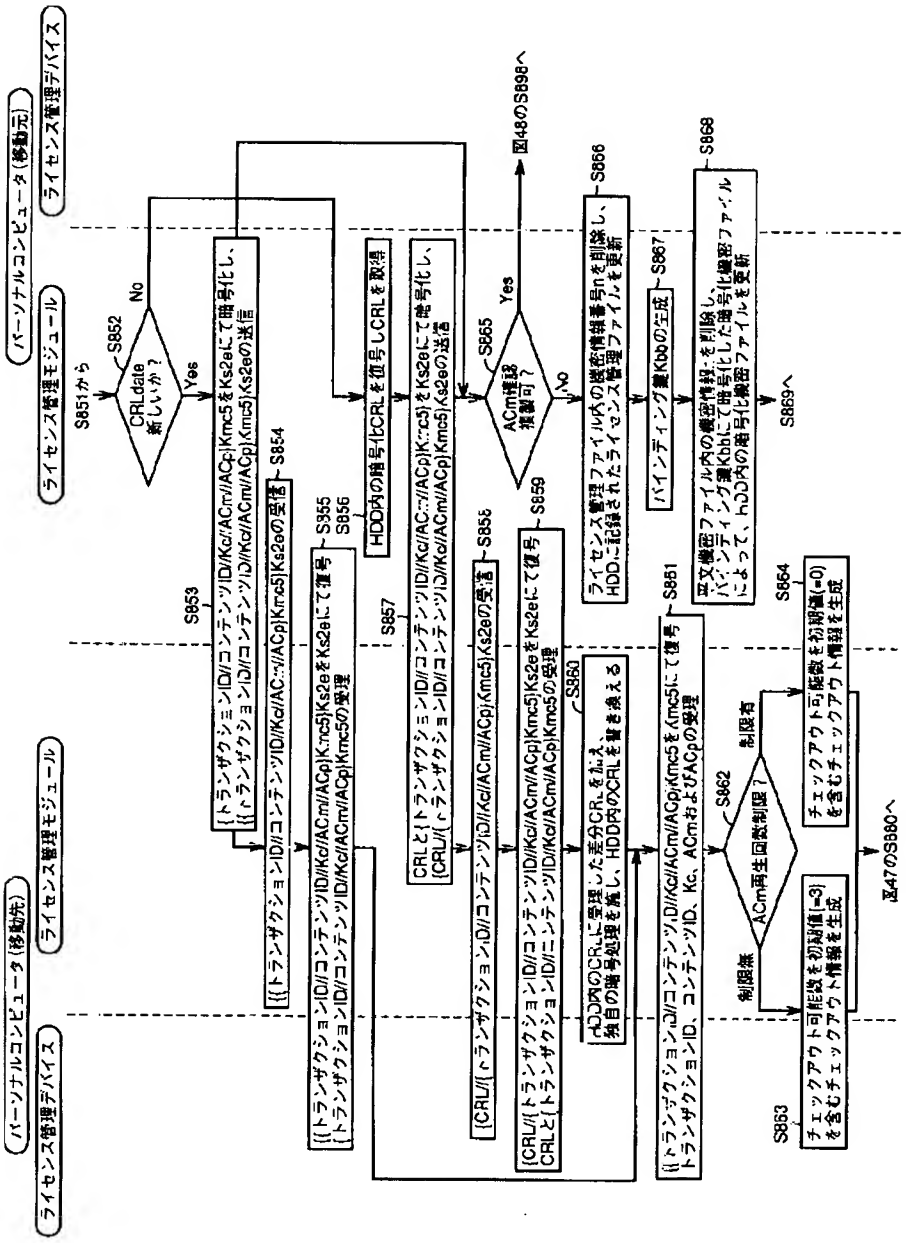
【図57】


ライセンス管理モジュール
ライセンス管理デバイス
開始
ウォータマークの利用規則を検出
S700
複製
S701
複製不可
利用規則制有り
利用規則無し
S705
ライセンス再製禁止・移動禁止且つ再生回数無制限なACm/無期限通常再生可能なACpを割り当てる
音楽CDからデータを取り込み、複製条件を変更したウォータマークに付け替える
S702
利用規則を反映したACm.ACpの生成
S703
S706
チェックアウト可能数を初期値(=3)を含むチェックアウト情報を生成
利用規則を反映したチェックアウト可能数を含むチェックアウト情報生成
S704
ライセンス鍵Kcの生成
S707
トランザクションID、コンテンツIDを生成
S708
S733へ
S723aへ

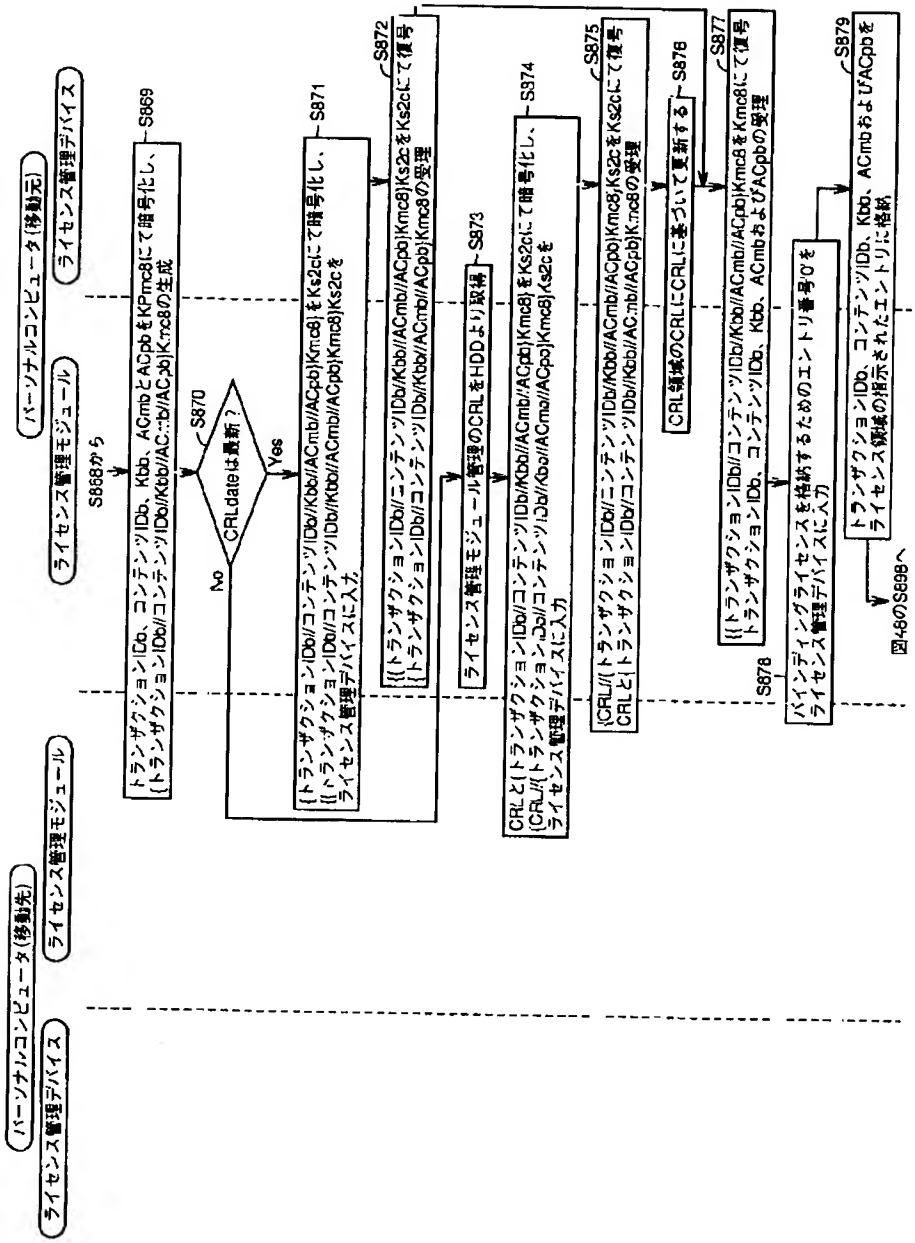
【図44】


パーソナルコンピュータ(移動先)
ライセンス管理デバイス
ライセンス管理モジュール
パーソナルコンピュータ(移動元)
ライセンス管理デバイス
ライセンス管理モジュール
S838から
S839
KPm5の受理
No
Yes
S840
Cm5 ≠ CRL
No
Yes
S903へ
S841
セッション鍵Ks2dの生成
S842
KPm5にてKs2dを暗号化し、{Ks2d}Km5の生成
S843
トランザクションID//{Ks2d}Km5の送信
S844
トランザクションID//{Ks2d}Km5の受信
S845
{Ks2d}Km5を受けて、Km5にて復号し、Ks2dの受理
S846
セッション鍵Ks2eの生成
S847
HDD内の暗号化CRLを復号しCRLを取得、HDDから取得したCRLからCRLdateを取得
S848
Ks2e、KPmc5とCRLdataをKs2dにて暗号化し、{Ks2e//KPmc5//CRLdate}Ks2dの送信
S849
{Ks2e//KPmc5//CRLdate}Ks2dを受信
S850
{Ks2e//KPmc5//CRLdate}Ks2dをKs2dにて復号し、Ks2e、KPmc5およびCRLdateの受理
S851
トランザクションID、ニンテンツID、Kc、ACmおよびACpをKPmc5にて暗号化し、{トランザクションID//コンテンツID//Kc//ACm//ACp}K::c5を生成
S852へ

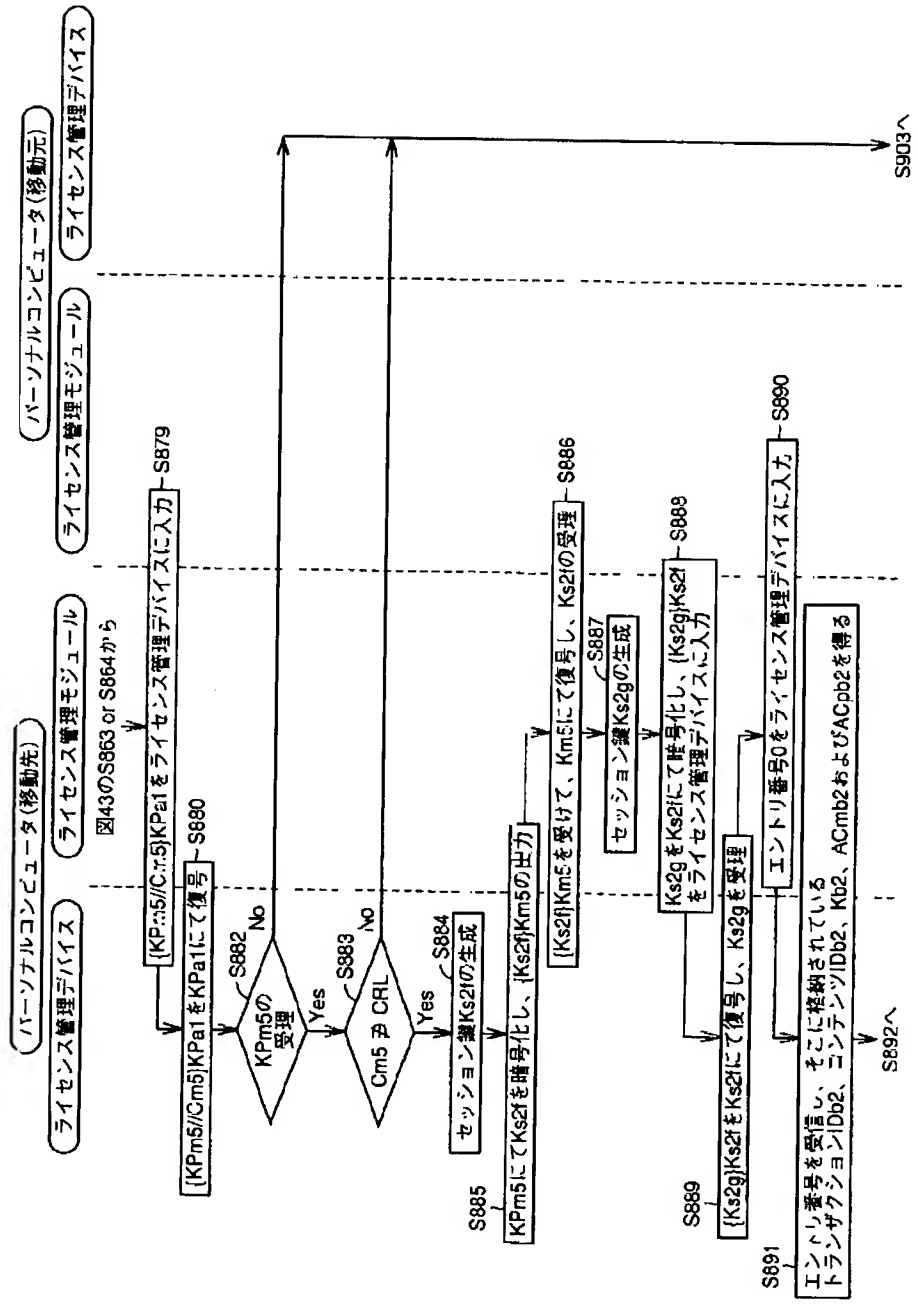
【図45】


パーソナルコンピュータ(移動先)
ライセンス管理デバイス
ライセンス管理モジュール
パーソナルコンピュータ(移動元)
ライセンス管理モジュール
ライセンス管理デバイス
S851から
S852
CRLdate新しいか？
No
Yes
S853
{{トランザクションID//コンテンツID//Kci//ACm//ACp}Kmc5をKs2eにて暗号化し、
{{トランザクションID//コンテンツID//Kci//ACm//ACp}Kmc5}Ks2eの送信
S854
{{トランザクションID//コンテンツID//Kci//ACm//ACp}Kmc5}Ks2eの受信
S855
ACm情報複製可？
Yes
No
図48のS898へ
S856
{{トランザクションID//コンテンツID//Kci//ACm//ACp}Kmc5}Ks2eをKs2eにて復号
S857
HDD内の暗号化CRLを復号しCRLを取得
S858
CRLと{{トランザクションID//コンテンツID//Kci//AC::://ACp}Kmc5}Ks2eにて暗号化し、
{CRL//{{トランザクションID//Kci//ACm//ACp}Kmc5}Ks2eの送信
S859
{CRL//{{トランザクションID//コンテンツID//Kci//ACm//ACp}Kmc5}Ks2eをKs2eにて復号
CRLと{{トランザクションID//コンテンツID//Kci//ACm//ACp}Kmc5の受理
S860
HDD内のCRLに受理した差分CRLをみよ、
旧目の暗号処理を残し、HDD内のCRLを置き換える
S861
{{トランザクションID//コンテンツID//Kci//ACm//ACp}Kmc5にて復号
トランザクションID、コンテンツID、Kc、ACmおよびACpの受理
S862
ACm再生回数制限？
制限無
制限有
S863
チェックアウト可能数を初期値{=3}
を含むチェックアウト情報を生成
S864
チェックアウト可能数を初期値{=0}
を含むチェックアウト情報を生成
図47のS880へ
S865
ライセンス管理ファイル内の機密情報事項nを削除し、
HDDに記録されたライセンス管理ファイルを更新
S866
バインディング鍵Kbbの生成
S867
S868
平文機密ファイル内の機密情報・を判別し、
バインディング鍵Kbbにて暗号化した暗号化機密ファイル
によって、HDD内の暗号化機密ファイルを更新
S869へ

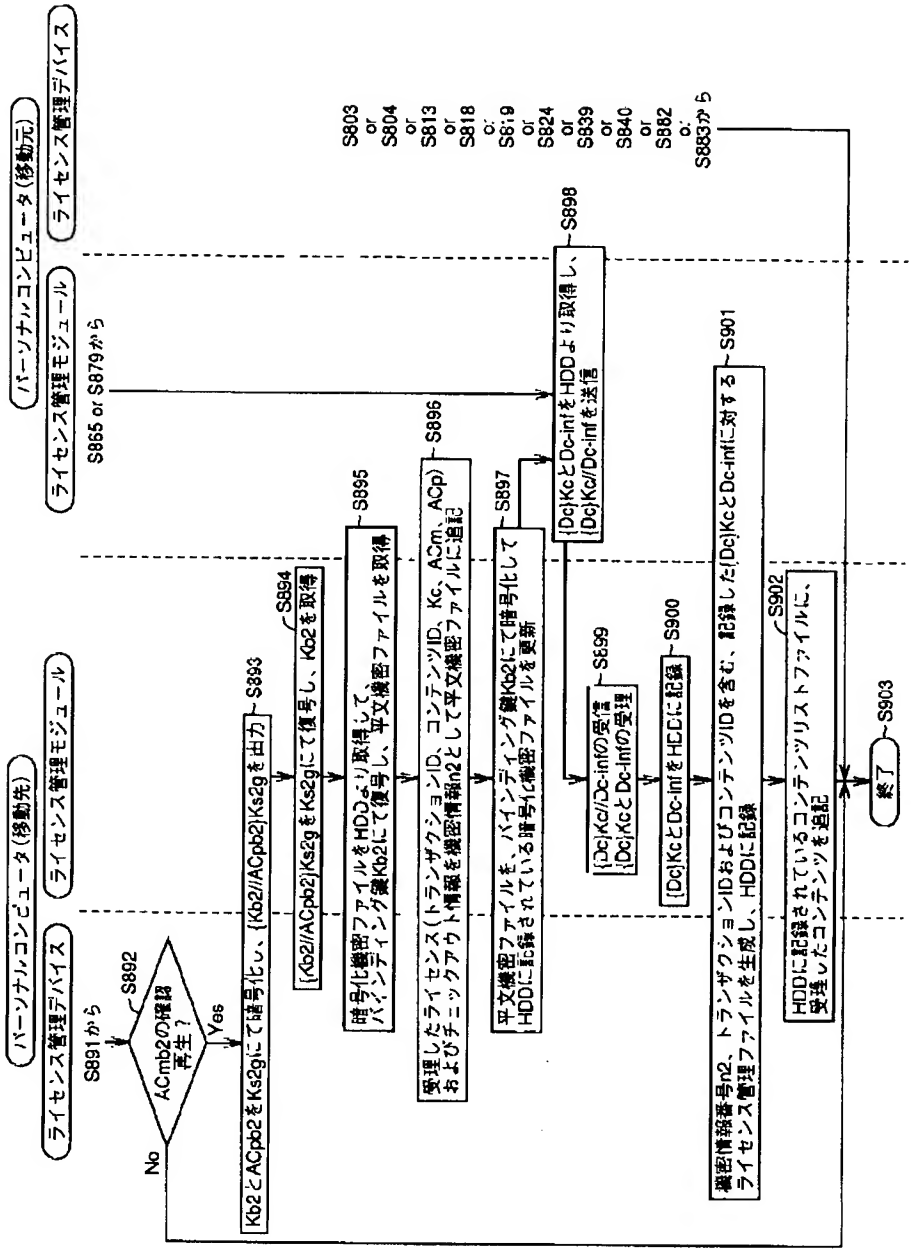
【図46】


パーソナルコンピュータ(移動先)
ライセンス管理デバイス
ライセンス管理モジュール
パーソナルコンピュータ(移動元)
ライセンス管理モジュール
ライセンス管理デバイス
S868から
トランザクションIDb、Kbb、ACmbとACpbをKPmc8にて暗号化し、
{{トランザクションIDb//Kbb//AC::b//ACpb}K::c8の生成
S869
S870
CRLdateは最新?
No
Yes
{トランザクションIDb//コンテンツIDb//Kbb//ACmb//ACpb}Kmc8}をKs2cにて暗号化し、
{{トランザクションIDb//コンテンツIDb//Kbb//ACmb//ACpb}Kmc8}Ks2cを
ライセンス管理デバイスに入力
S871
{{トランザクションIDb//コンテンツIDb//Kbb//ACmb//ACpb}Kmc8}Ks2cをKs2cにて復号
{{トランザクションIDb//コンテンツIDb//Kbb//ACmb//ACpb}Kmc8の受理
S872
ライセンス管理モジュールCRLをHDDより取得
S873
CRLと{トランザクションIDb//コンテンツIDb//Kbb//ACmb//ACpb}Kmc8}をKs2cにて暗号化し、
{CRL//{トランザクションIDb//コンテンツIDb//Kbb//ACmb//ACpb}Kmc8}Ks2cを
ライセンス管理デバイスに入力
S874
{CRL//{トランザクションIDb//コンテンツIDb//Kbb//ACmb//ACpb}Kmc8}Ks2cをKs2cにて復号
CRLと{トランザクションIDb//コンテンツIDb//Kbb//AC::b//ACpb}K::c8の受理
S875
CRL領域のCRLにCRLに基づいて更新する
S876
{{トランザクションIDb//コンテンツIDb//Kbb//ACmb//ACpb}Kmc8}をKmc8にて復号
トランザクションIDb、コンテンツIDb、Kbb、ACmbおよびACpbの受理
S877
S878
バインディングライセンスを格納するためのエントリ番号'0'を
ライセンス管理デバイスに入力
S879
トランザクションIDb、コンテンツIDb、Kbb、ACmbおよびACpbを
ライセンス領域の指示されたエントリに格納
図48のS898へ

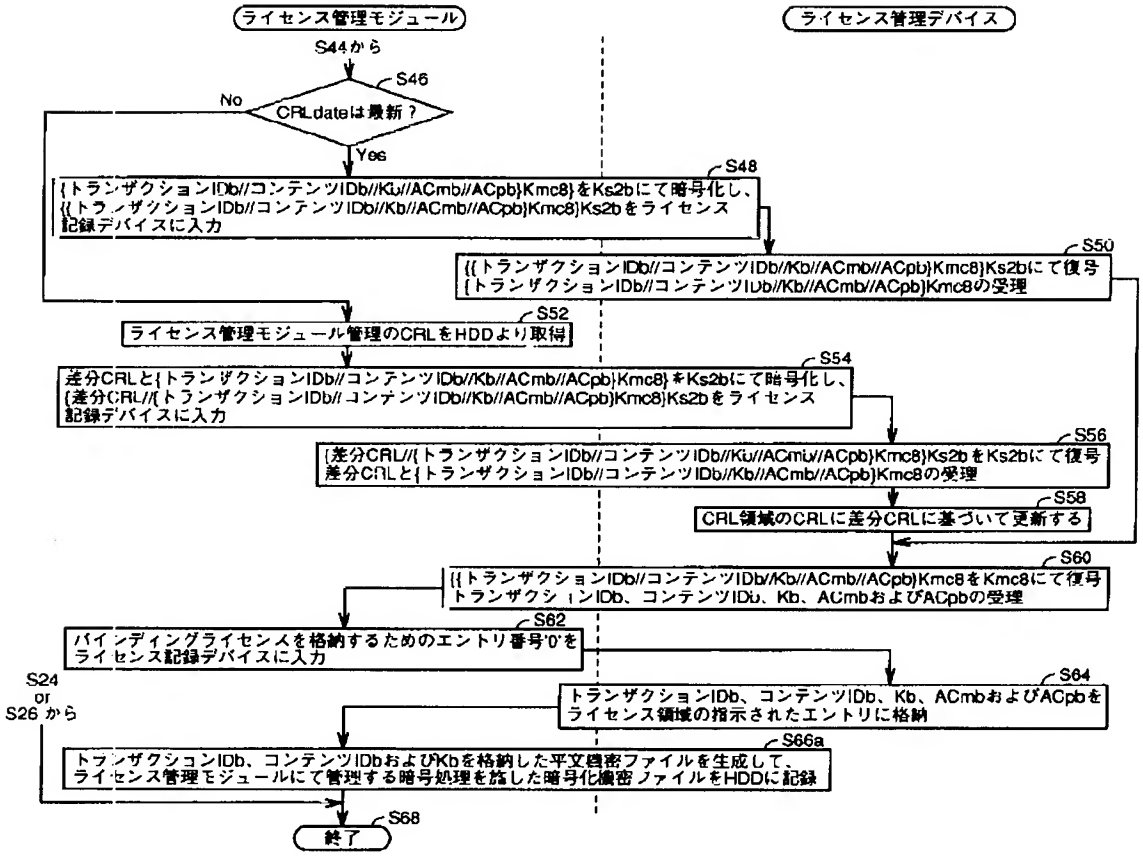
【図47】


パーソナルコンピュータ(移動先)
ライセンス管理デバイス
ライセンス管理モジュール
パーソナルコンピュータ(移動元)
ライセンス管理モジュール
ライセンス管理デバイス
図43のS863 or S864から
[KPm5//Cm5]KPa1をライセンス管理デバイスに入力 S879
[KPm5//Cm5]KPa1をKPa1にて復号 S880
S882 KPm5の受理 No Yes
S883 Cm5 ≠ CRL No Yes
S884 セッション鍵Ks2iの生成
S885 KPm5にてKs2iを暗号化し、[Ks2i]Km5の出力
[Ks2i]Kmを受けて、Km5にて復号し、Ks2iの受理 S886
S887 セッション鍵Ks2gの生成
Ks2gをKs2iにて暗号化し、[Ks2g]Ks2iをライセンス管理デバイスに入力 S888
S889 [Ks2g]Ks2iをKs2iにて復号し、Ks2gを受理
エントリ番号0をライセンス管理デバイスに入力 S890
S891 エントリ番号を受信し、そこに格納されているトランザクションIDb2、コンテンツIDb2、Kb2、ACmb2およびACpb2を得る
S892へ
S903へ

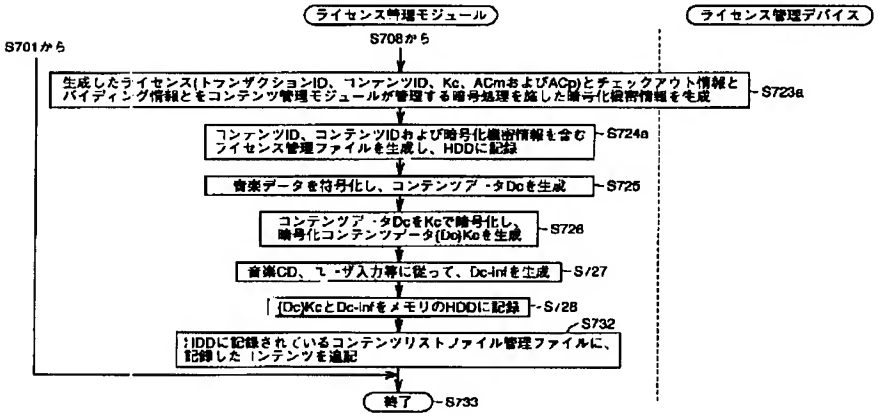
【図48】


パーソナルコンピュータ(移動先)
ライセンス管理デバイス
ライセンス管理モジュール
パーソナルコンピュータ(移動元)
ライセンス管理モジュール
ライセンス管理デバイス
S891から
S892
ACmb2の確認
再生?
No
Yes
S865 or S879から
S803 or S804 or S813 or S818 or S819 or S824 or S839 or S840 or S882 or S883から
Kb2とACpb2をKs2gにて暗号化し、{Kb2//ACpb2|Ks2gを出力
S893
{Kb2//ACpb2|Ks2gをKs2gにて復号し、Kb2を取得
S894
暗号化機密ファイルをHDDより取得して
バインディング鍵Kb2にて復号し、平文機密ファイルを取得
S895
受理したライセンス(トランザクションID、コンテンツID、Kc、ACm、ACp)
およびチニックアウト情報を機密情報in2として平文機密ファイルに追記
S896
平文機密ファイルを、バインディング鍵Kb2にて暗号化して
HDDに記録されている暗号化機密ファイルを更新
S897
{Dc|KcとDc-infをHDDより取得し、
{Dc|Kc//Dc-infを送信
S898
{Dc|Kc//Dc-infの受信
{Dc|KcとDc-infの受理
S899
{Dc|KcとDc-infをHDDに記録
S900
機密情報番号in2、トランザクションIDおよびコンテンツIDを含む、記録した{Dc|KcとDc-infに対する
ライセンス管理ファイルを生成し、HDDに記録
S901
HDDに記録されているコンテンツリストファイルに、
受理したコンテンツを追記
S902
終了
S903

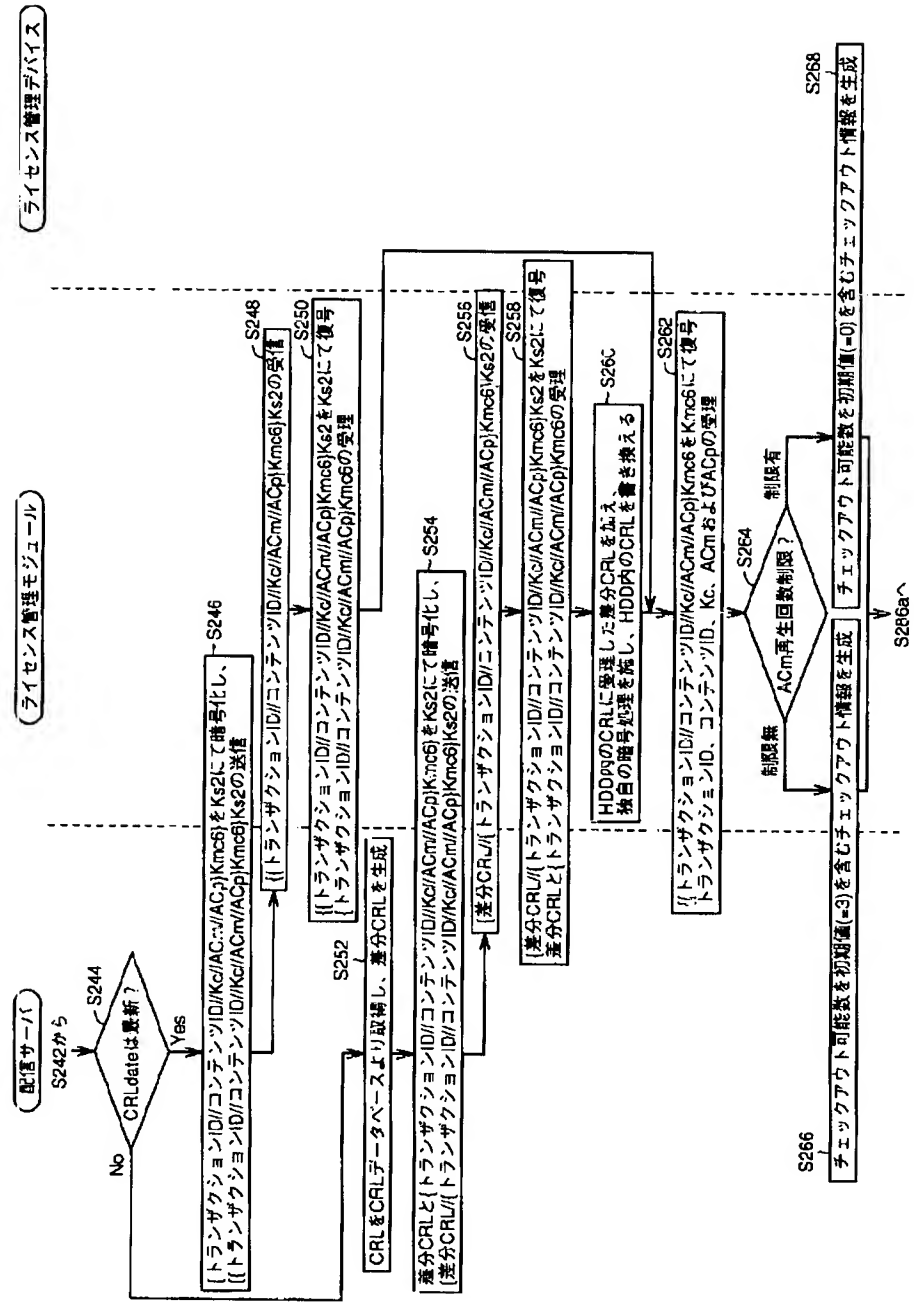
【図52】


ライセンス管理モジュール
ライセンス管理デバイス
S44から
S46
No
CRLdateは最新？
Yes
S48
{トランザクションIDb//コンテンツIDb//Ku//ACmb//ACpb}Kmc8}をKs2bにて暗号化し、
{{トランザクションIDb//コンテンツIDb//Kb//ACmb//ACpb}Kmc8}Ks2bをライセンス
記録デバイスに入力
S50
{{トランザクションIDb//コンテンツIDb//Kb//ACmb//ACpb}Kmc8}Ks2bにて復号
{トランザクションIDb//コンテンツIDb//Kb//ACmb//ACpb}Kmc8の受理
S52
ライセンス管理モジュール管理のCRLをHDDより取得
S54
差分CRLと{トランザクションIDb//コンテンツIDb//Kb//ACmb//ACpb}Kmc8}＊Ks2bにて暗号化し、
{差分CRL//{トランザクションIDb//コンテンツIDb//Kb//ACmb//ACpb}Kmc8}Ks2bをライセンス
記録デバイスに入力
S56
{差分CRL//{トランザクションIDb//コンテンツIDb//Ku//ACmb//ACpb}Kmc8}Ks2bをKs2bにて復号
差分CRLと{トランザクションIDb//コンテンツIDb//Kb//ACmb//ACpb}Kmc8の受理
S58
CRL領域のCRLに差分CRLに基づいて更新する
S60
{{トランザクションIDb//コンテンツIDb//Kb//ACmb//ACpb}Kmc8をKmc8にて復号
トランザクションIDb、コンテンツIDb、Kb、ACmbおよびACpbの受理
S62
バインディングライセンスを格納するためのエントリ番号'0'を
ライセンス記録デバイスに入力
S24
or
S26から
S64
トランザクションIDb、コンテンツIDb、Kb、ACmbおよびACpbを
ライセンス領域の指示されたエントリに格納
S66a
トランザクションIDb、コンテンツIDbおよびKbを格納した平文機密ファイルを生成して、
ライセンス管理モジュールにて管理する暗号処理を施した暗号化機密ファイルをHDDに記録
S68
終了

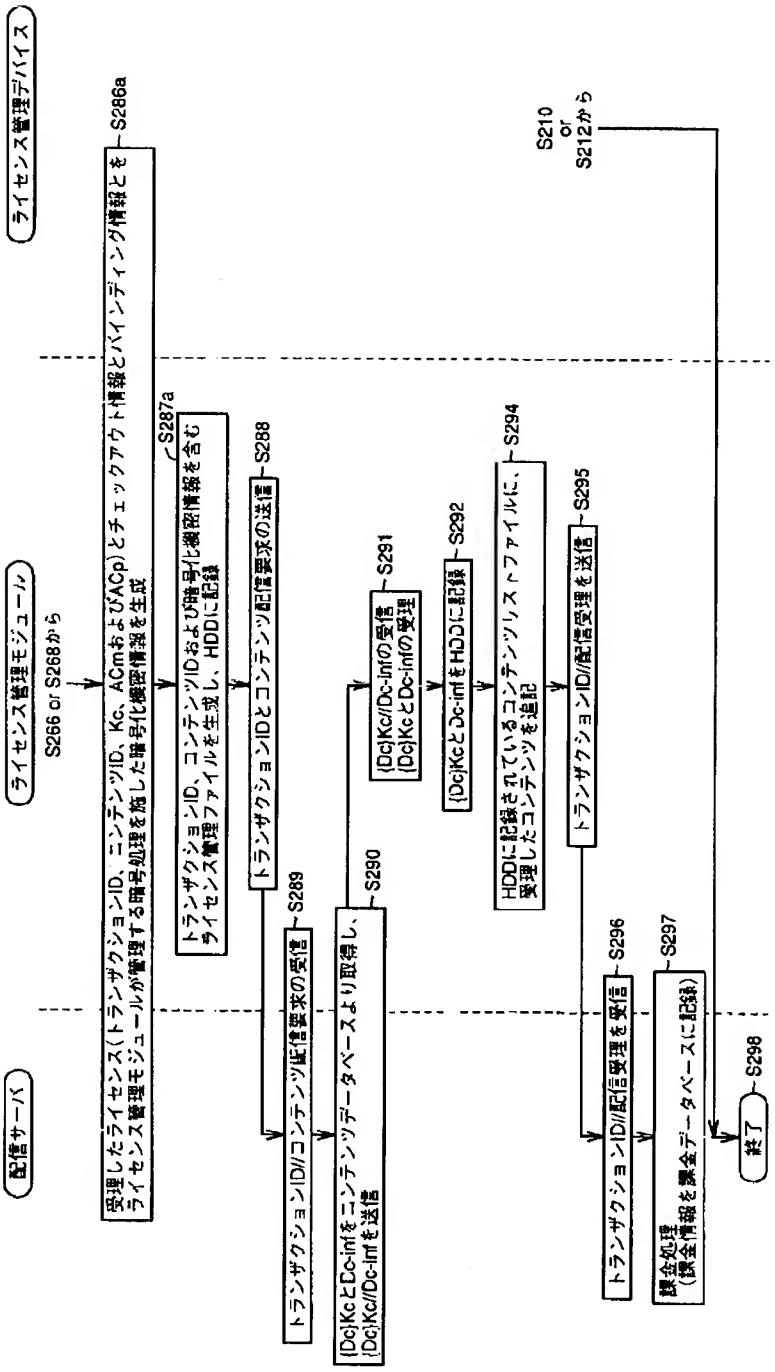
【図58】


ライセンス管理モジュール
ライセンス管理デバイス
S701から
S708から
生成したライセンス(トランザクションID、コンテンツID、Kc、ACmおよびACp)とチェックアウト情報と
バインディング情報とをコンテンツ管理モジュールが管理する暗号処理を施した暗号化機密情報を生成
S723a
コンテンツID、コンテンツIDおよび暗号化機密情報を含む
ライセンス管理ファイルを生成し、HDDに記録
S724a
音楽データを符号化し、コンテンツデータDcを生成
S725
コンテンツデータDcをKcで暗号化し、
暗号化コンテンツデータ{Dc}Kcを生成
S726
音楽CD、ユーザ入力等に従って、Dc-Infを生成
S727
{Dc}KcとDc-Infをメモリ→HDDに記録
S728
HDDに記録されているコンテンツリストファイル管理ファイルに、
記録したコンテンツを追記
S732
終了
S733

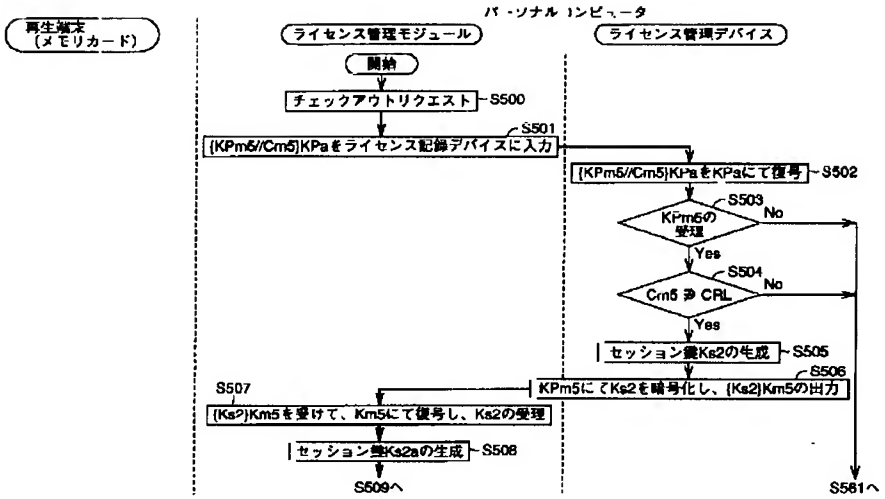
【図55】


配信サーバ
ライセンス管理モジュール
ライセンス管理デバイス
S242から
S244
CRLdateは最新？
No
Yes
S246
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc6}Ks2の送信
S248
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc6}Ks2の受信
S250
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc6}Ks2をKs2にて復号
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc6}Ks2の受理
S252
CRLをCRLデータベースより取得し、差分CRLを生成
S254
差分CRLと{トランザクションID//Kc//ACm//ACp}Kmc6をKs2にて暗号化し、
差分CRLと{トランザクションID//Kc//ACm//ACp}Kmc6}Ks2の送信
S256
{差分CRLと{トランザクションID//Kc//ACm//ACp}Kmc6}Ks2の受信
S258
{差分CRLと{トランザクションID//Kc//ACm//ACp}Kmc6}Ks2をKs2にて復号
差分CRLと{トランザクションID//Kc//ACm//ACp}Kmc6の受理
S26C
HDD内のCRLに登録した差分CRLを加え、
独自の暗号処理を施し、HDD内のCRLを書き換える
S262
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc6をKmc6にて復号
トランザクションID、コンテンツID、Kc、ACmおよびACpの受理
S264
ACm再生回数制限？
制限有
制限無
S266
チェックアウト可能数を初期値(=3)を含むチェックアウト情報を生成
S268
チェックアウト可能数を初期値(=0)を含むチェックアウト情報を生成
S286aへ

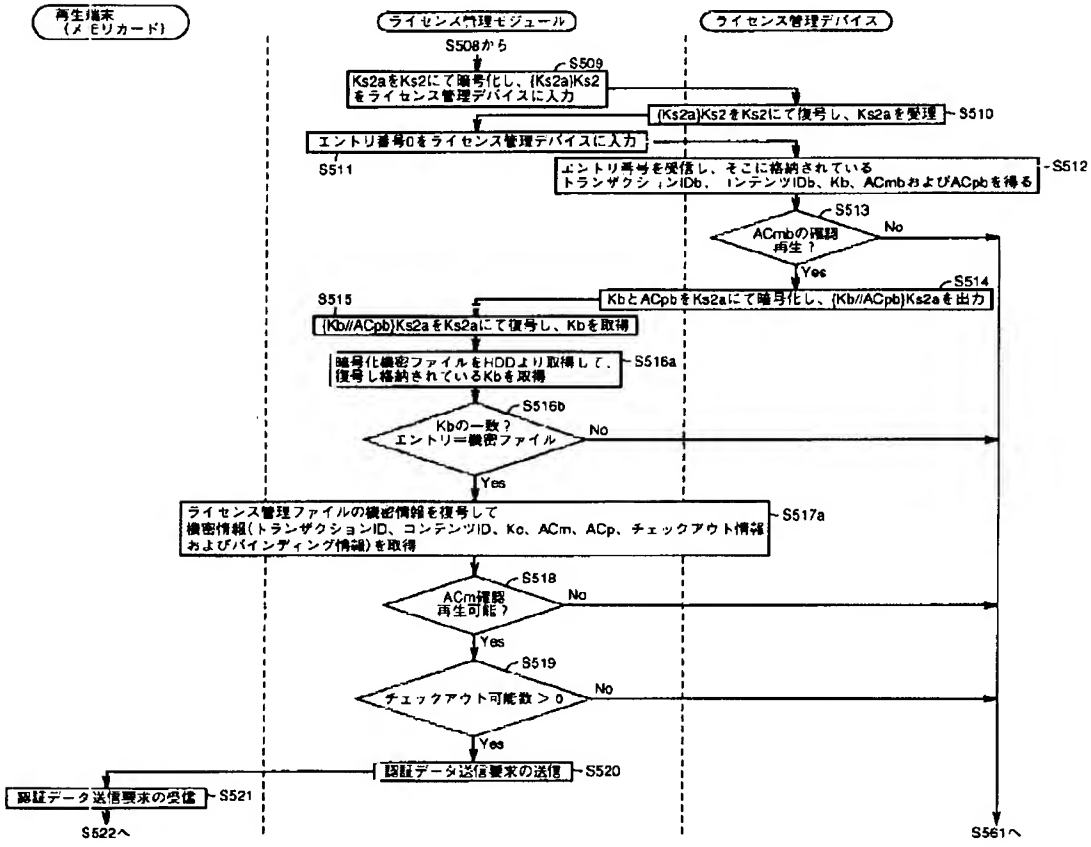
【図56】


配信サーバ
ライセンス管理モジュール
ライセンス管理デバイス
S266 or S268から
受理したライセンス(トランザクションID、コンテンツID、Kc、ACmおよびACp)とチェックアウト情報とバインディング情報とを
ライセンス管理モジュールが管理する暗号処理を施した暗号化機密情報を生成
S286a
トランザクションID、コンテンツIDおよび暗号化機密情報を含む
ライセンス管理ファイルを生成し、HDDに記録
S287a
トランザクションIDとコンテンツ配信要求の送信
S288
トランザクションID//コンテンツ配信要求の受信
S289
{Dc}KcとDc-infをコンテンツデータベースより取得し、
{Dc}Kc//Dc-infを送信
S290
{Dc}Kc//Dc-infの受信
{Dc}KcとDc-infの処理
S291
{Dc}KcとDc-infをHDDに記録
S292
HDDに記録されているコンテンツリストファイルに、
受理したコンテンツを追記
S294
トランザクションID//配信受理を送信
S295
S210
or
S212から
トランザクションID//配信受理を受信
S296
課金処理
(課金情報を課金データベースに記録)
S297
終了
S298

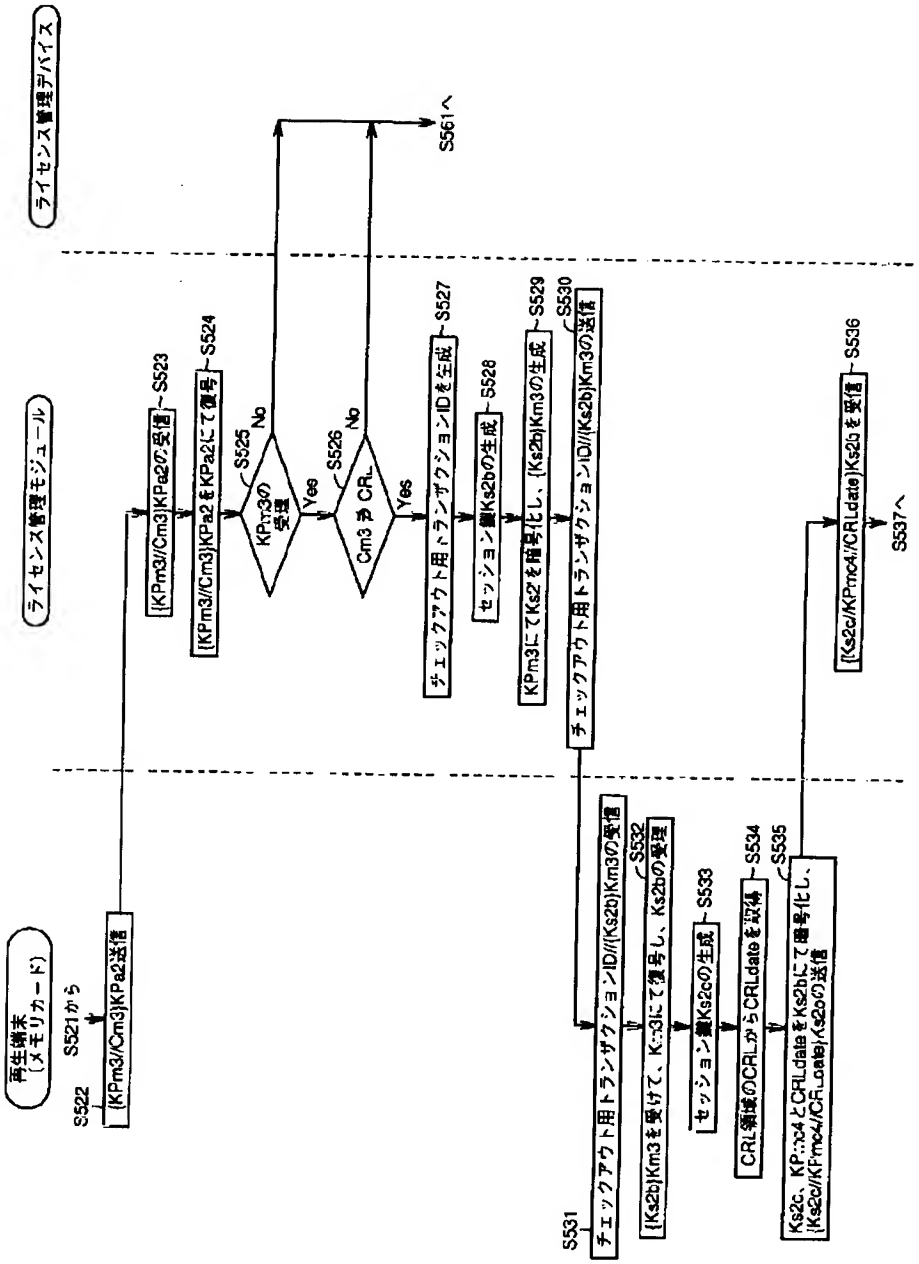
【図59】


パーソナルコンピュータ
再生端末(メモリカード)
ライセンス管理モジュール
ライセンス管理デバイス
開始
チェックアウトリクエスト
S500
S501
{KPm5//Cm5}KPaをライセンス記録デバイスに入力
{KPm5//Cm5}KPaをKPaにて復号
S502
S503
Kpm5の整理
No
Yes
S504
Cm5 ∋ CRL
No
Yes
セッション鍵Ks2の生成
S505
S506
KPm5にてKs2を暗号化し、{Ks2}Km5の出力
S507
{Ks2}Km5を受けて、Km5にて復号し、Ks2の受理
セッション鍵Ks2aの生成
S508
S509へ
S561へ

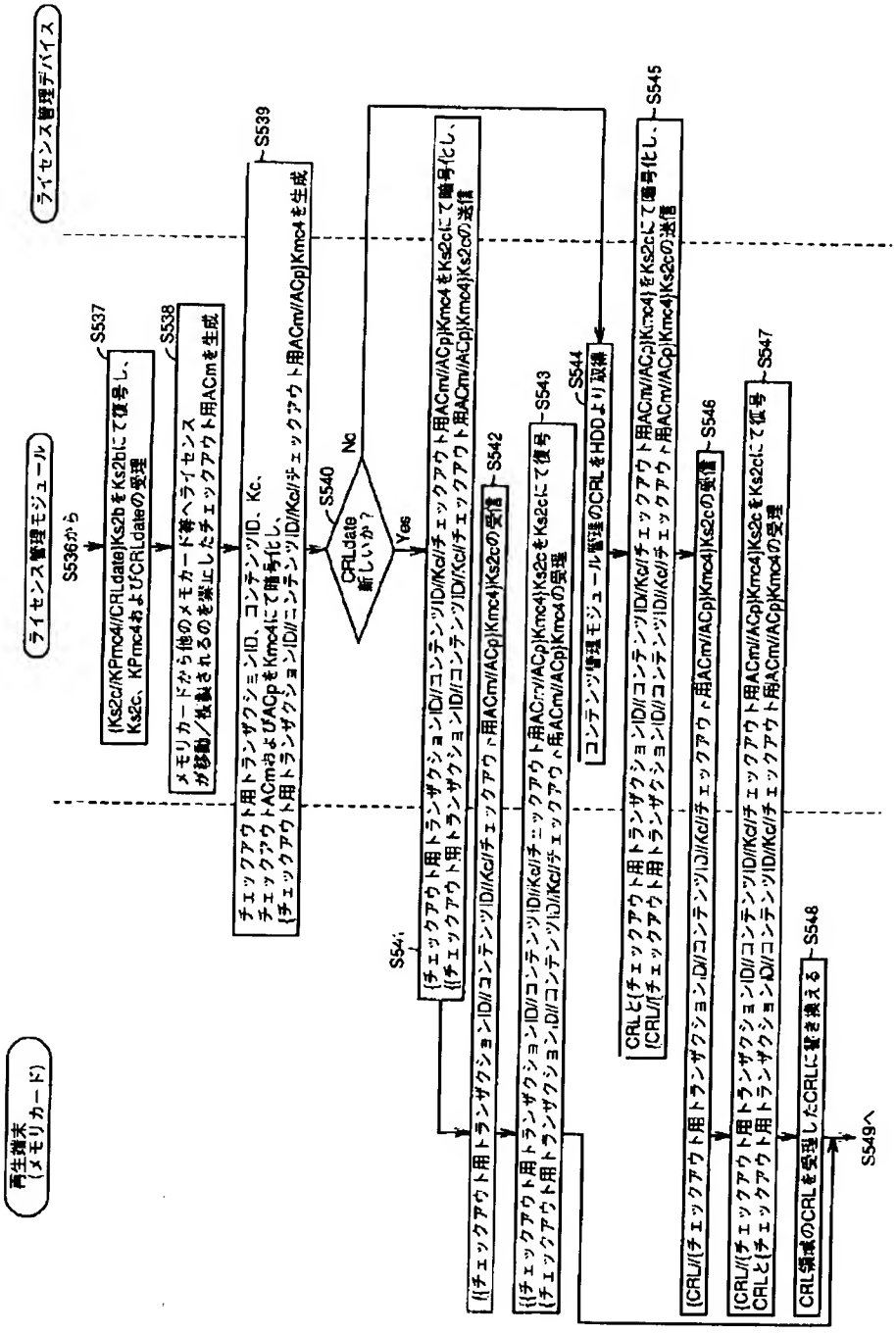
【図60】


再生端末(メモリカード)
ライセンス管理モジュール
ライセンス管理デバイス
S508から
S509
Ks2aをKs2にて暗号化し、{Ks2a}Ks2をライセンス管理デバイスに入力
{Ks2a}Ks2をKs2にて復号し、Ks2aを受理
S510
エントリ番号0をライセンス管理デバイスに入力
S511
エントリ番号を受信し、そこに格納されているトランザクションIDb、コンテンツIDb、Kb、ACmbおよびACpbを得る
S512
S513
ACmbの種類再生？
No
Yes
S514
KbとACpbをKs2aにて暗号化し、{Kb//ACpb}Ks2aを出力
S515
{Kb//ACpb}Ks2aをKs2aにて復号し、Kbを取得
暗号化機密ファイルをHDDより取得して、復号し格納されているKbを取得
S516a
S516b
Kbの一致？エントリ＝機密ファイル
No
Yes
ライセンス管理ファイルの機密情報を復号して機密情報(トランザクションID、コンテンツID、Kc、ACm、ACp、チェックアウト情報およびバインディング情報)を取得
S517a
S518
ACm種類再生可能？
No
Yes
S519
チェックアウト可能数＞0
No
Yes
認証データ送信要求の送信
S520
認証データ送信要求の受信
S521
S522へ
S561へ

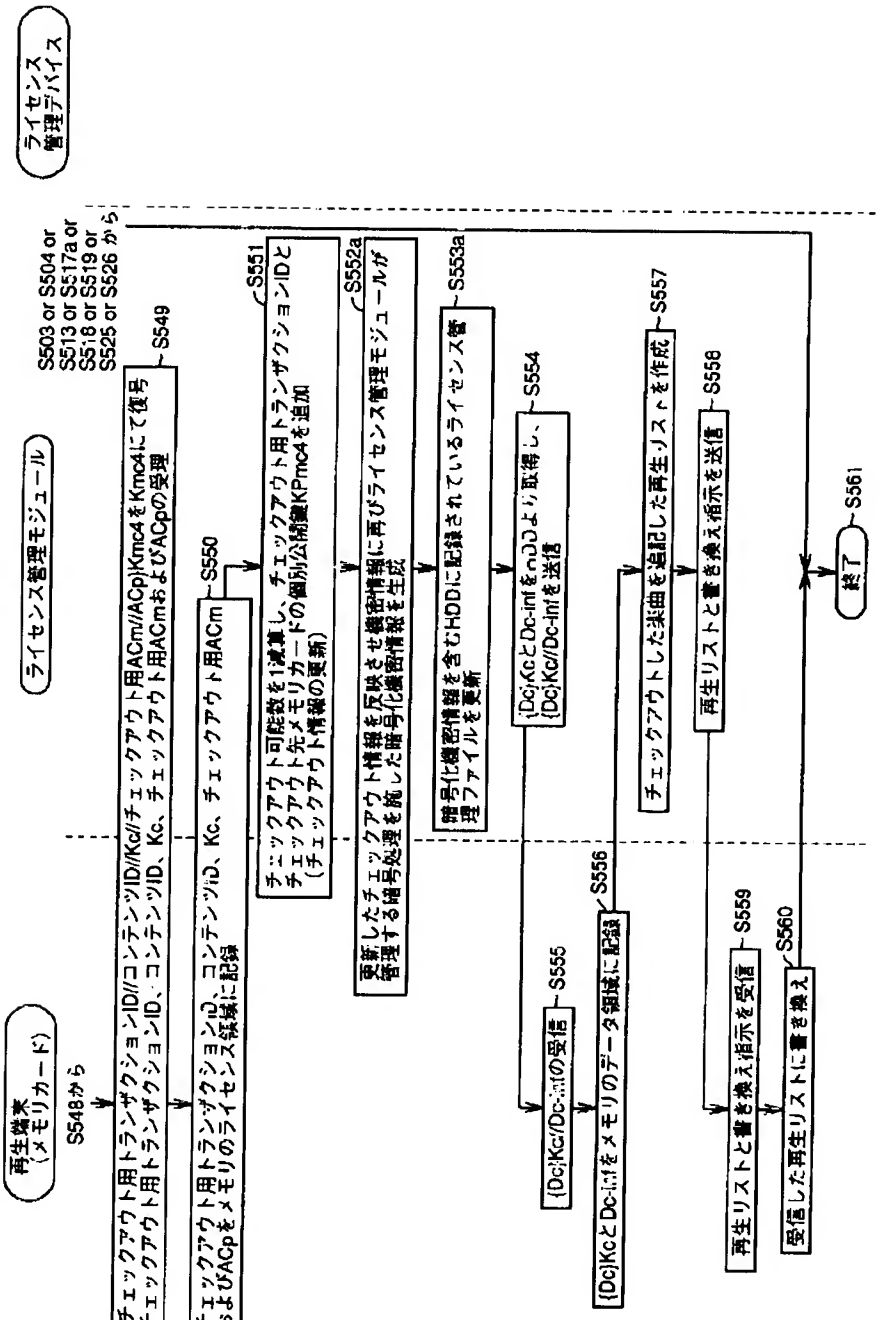
【図61】


再生端末
(メモリカード)
ライセンス管理モジュール
ライセンス管理デバイス
S521から
S522
{KPm3/(Cm3)KPa2送信
S523
{KPm3/(Cm3)KPa2の受信
S524
{KPm3/(Cm3)KPa2をKPa2にて復号
S525
KPm3の受理
No
Yes
S526
Cm3 ≠ CRL
No
Yes
S561へ
S527
チェックアウト用トランザクションIDを生成
S528
セッション鍵Ks2bの生成
S529
KPm3にてKs2'を暗号化し、{Ks2b}Km3の生成
S530
チェックアウト用トランザクションID//{Ks2b}Km3の送信
S531
チェックアウト用トランザクションID//{Ks2b}Km3の受信
S532
{Ks2b}Km3を受けて、Km3にて復号し、Ks2bの受理
S533
セッション鍵Ks2cの生成
S534
CRL領域のCRLからCRLdateを取得
S535
Ks2c、KPm4とCRLdateをKs2bにて暗号化し、
{Ks2c//KPm4//CRLdate}Ks2bの送信
S536
{Ks2c//KPm4//CRLdate}Ks2bを受信
S537へ

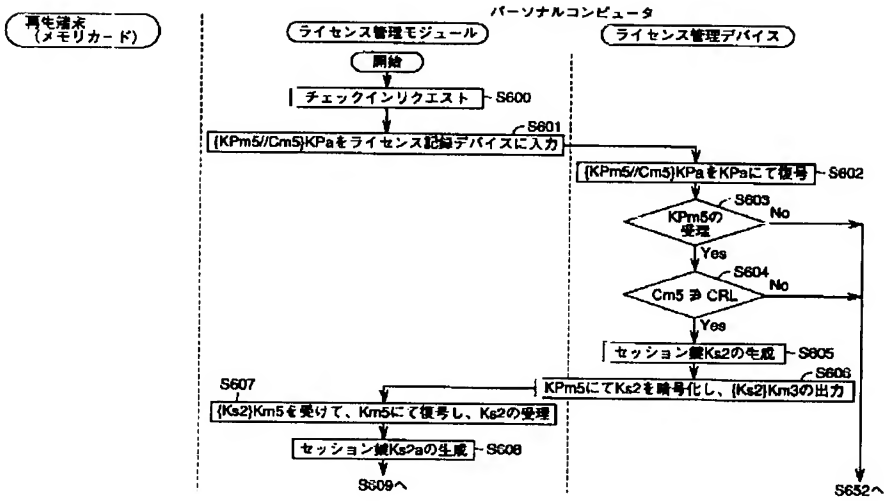
【図62】


再生端末
(メモリカード)
ライセンス管理モジュール
ライセンス管理デバイス
S536から
S537
{Ks2c/KPmc4/CRLdate}Ks2bをKs2bにて復号し、
Ks2c、KPmc4およびCRLdateの受理
S538
メモリカードから他のメモカード等へライセンス
が移動/複製されるのを禁止したチェックアウト用ACmを生成
S539
チェックアウト用トランザクションID、コンテンツID、Kc、
チェックアウトACmおよびACpをKmc4にて暗号化し、
{チェックアウト用トランザクションID//コンテンツID//Kc//チェックアウト用ACm//ACp}Kmc4を生成
S540
CRLdate
新しいか?
No
Yes
S541
{チェックアウト用トランザクションID//コンテンツID//Kc//チェックアウト用ACm//ACp}Kmc4をKs2cにて暗号化し、
{{チェックアウト用トランザクションID//コンテンツID//Kc//チェックアウト用ACm//ACp}Kmc4}Ks2cの送信
S542
{{チェックアウト用トランザクションID//コンテンツID//Kc//チェックアウト用ACm//ACp}Kmc4}Ks2cの受理
S543
{{チェックアウト用トランザクションID//コンテンツID//Kc//チェックアウト用ACm//ACp}Kmc4}Ks2cにて復号
{チェックアウト用トランザクションID//コンテンツID//Kc//チェックアウト用ACm//ACp}Kmc4の受理
S544
コンテンツ管理モジュール管理のCRLをHDDより取得
S545
CRLと{{チェックアウト用トランザクションID//コンテンツID//Kc//チェックアウト用ACm//ACp}Kmc4}をKs2cにて暗号化し、
{CRL//{{チェックアウト用トランザクションID//Kc//チェックアウト用ACm//ACp}Kmc4}Ks2cの送信
S546
{CRL//{チェックアウト用トランザクションID//Kc//チェックアウト用ACm//ACp}Kmc4}Ks2cの受理
S547
{CRL//{チェックアウト用トランザクションID//コンテンツID//Kc//チェックアウト用ACm//ACp}Kmc4}Ks2cをKs2cにて復号
CRLと{チェックアウト用トランザクションID//Kc//チェックアウト用ACm//ACp}Kmc4の受理
S548
CRL領域のCRLを受理したCRLに置き換える
S549へ

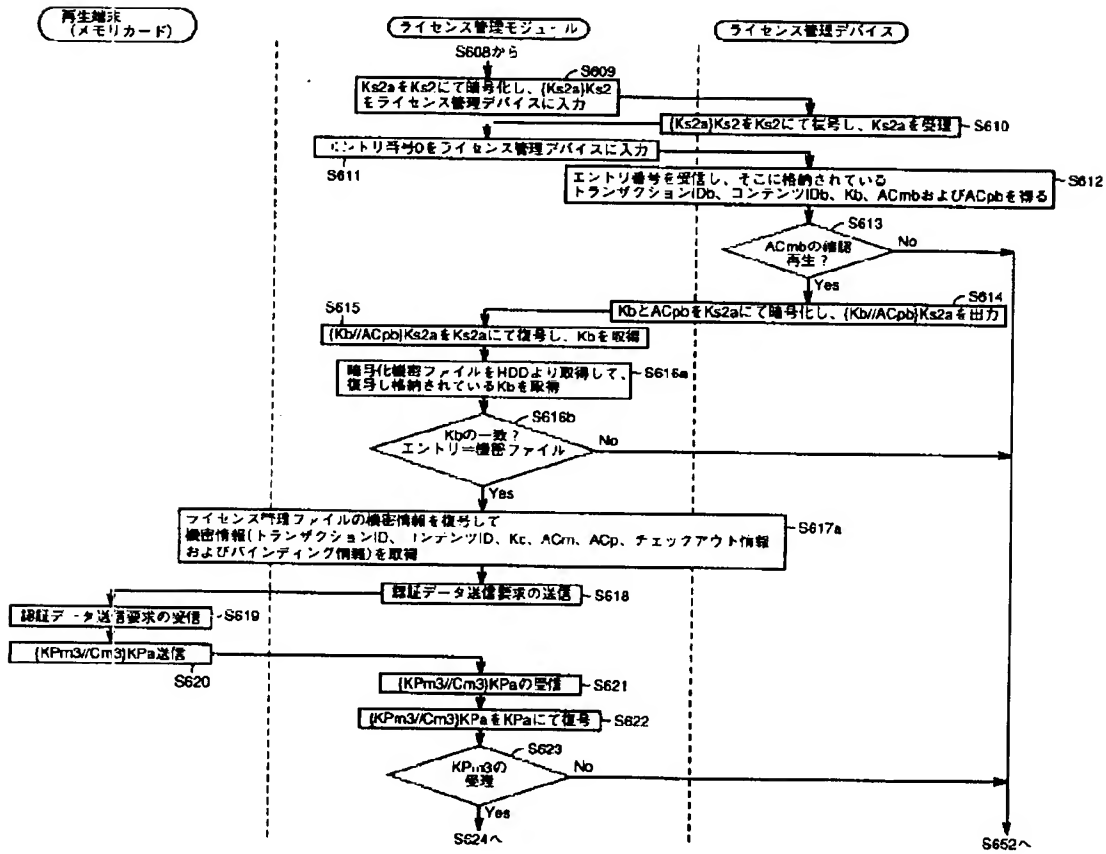
【図63】


再生端末
(メモリカード)
ライセンス管理モジュール
ライセンス
管理デバイス
S548から
S503 or S504 or
S513 or S517a or
S518 or S519 or
S525 or S526 から
{チェックアウト用トランザクションID//Kc//チェックアウト用ACm//ACp}Kmc4をKmc4にて復号
チェックアウト用トランザクションID、コンテンツID、Kc、チェックアウト用ACmおよびACpの受理
S549
チェックアウト用トランザクションID、コンテンツID、Kc、チェックアウト用ACm
およびACpをメモリのライセンス領域に記録
S550
チェックアウト可能数を1減算し、チェックアウト用トランザクションIDと
チェックアウト先メモリカードの個別公開鍵KPmc4を追加
(チェックアウト情報の更新)
S551
更新したチェックアウト情報を反映させ機密情報に再びライセンス管理モジュールが
管理する暗号処理を施した暗号化機密情報を生成
S552a
暗号化機密情報を含むHDDに記録されているライセンス管
理ファイルを更新
S553a
{Dc}Kcと Dc-inf をnDDより取得し、
{Dc}Kc//Dc-inf を送信
S554
{Dc}Kc//Dc-inf の受信
S555
{Dc}Kcと Dc-inf をメモリのデータ領域に記録
S556
チェックアウトした楽曲を追記した再生リストを作成
S557
再生リストと書き換え指示を送信
S558
再生リストと書き換え指示を受信
S559
受信した再生リストに書き換え
S560
終了
S561

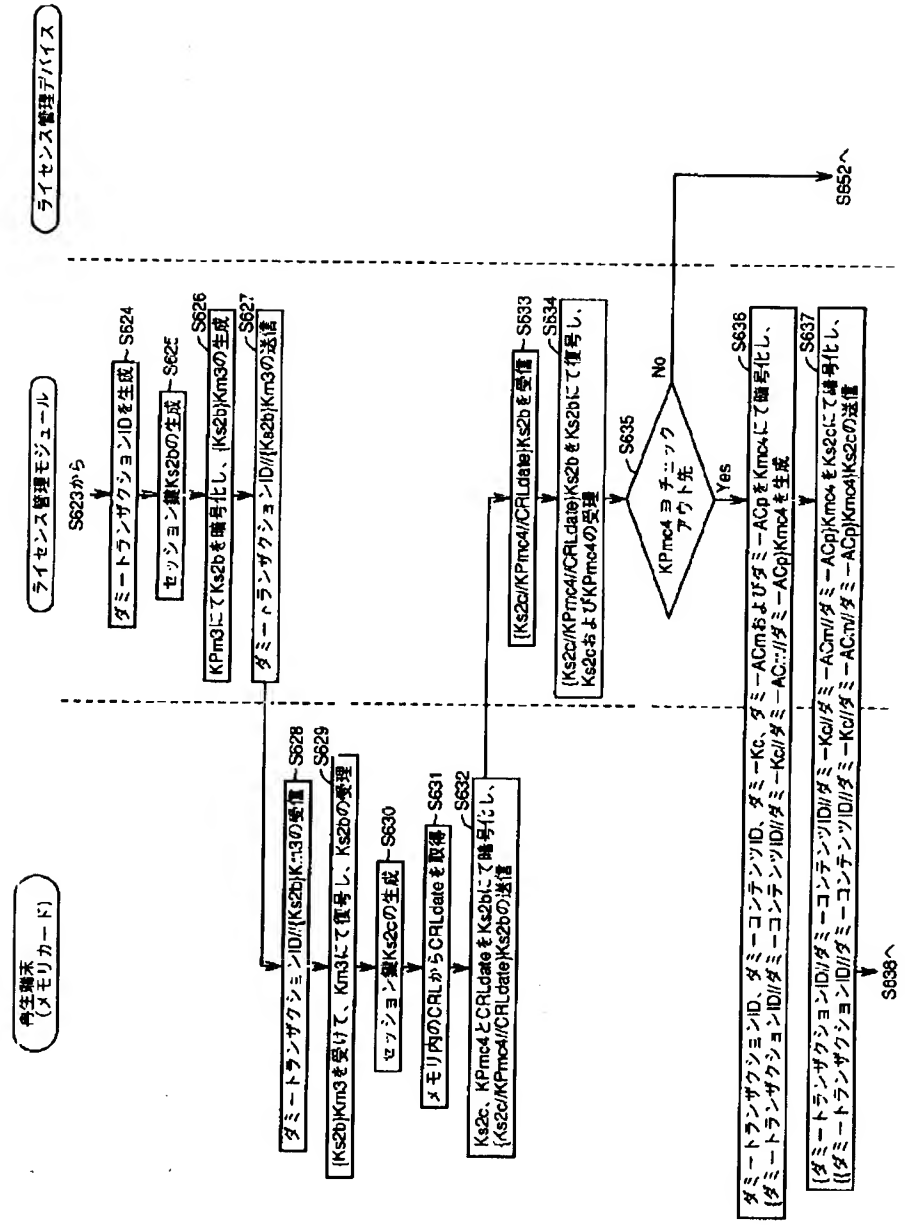
【図６４】


再生端末
(メモリカード)
パーソナルコンピュータ
ライセンス管理モジュール
ライセンス管理デバイス
開始
チェックインリクエスト
S600
S601
{KPm5//Cm5}KPaをライセンス記録デバイスに入力
{KPm5//Cm5}KPaをKPaにて復号
S602
S603
KPm5の受理
No
Yes
S604
Cm5 ∋ CRL
No
Yes
セッション鍵Ks2の生成
S605
S606
KPm5にてKs2を暗号化し、{Ks2}Km3の出力
S607
{Ks2}Km5を受けて、Km5にて復号し、Ks2の受理
セッション鍵Ks2aの生成
S608
S609へ
S652へ

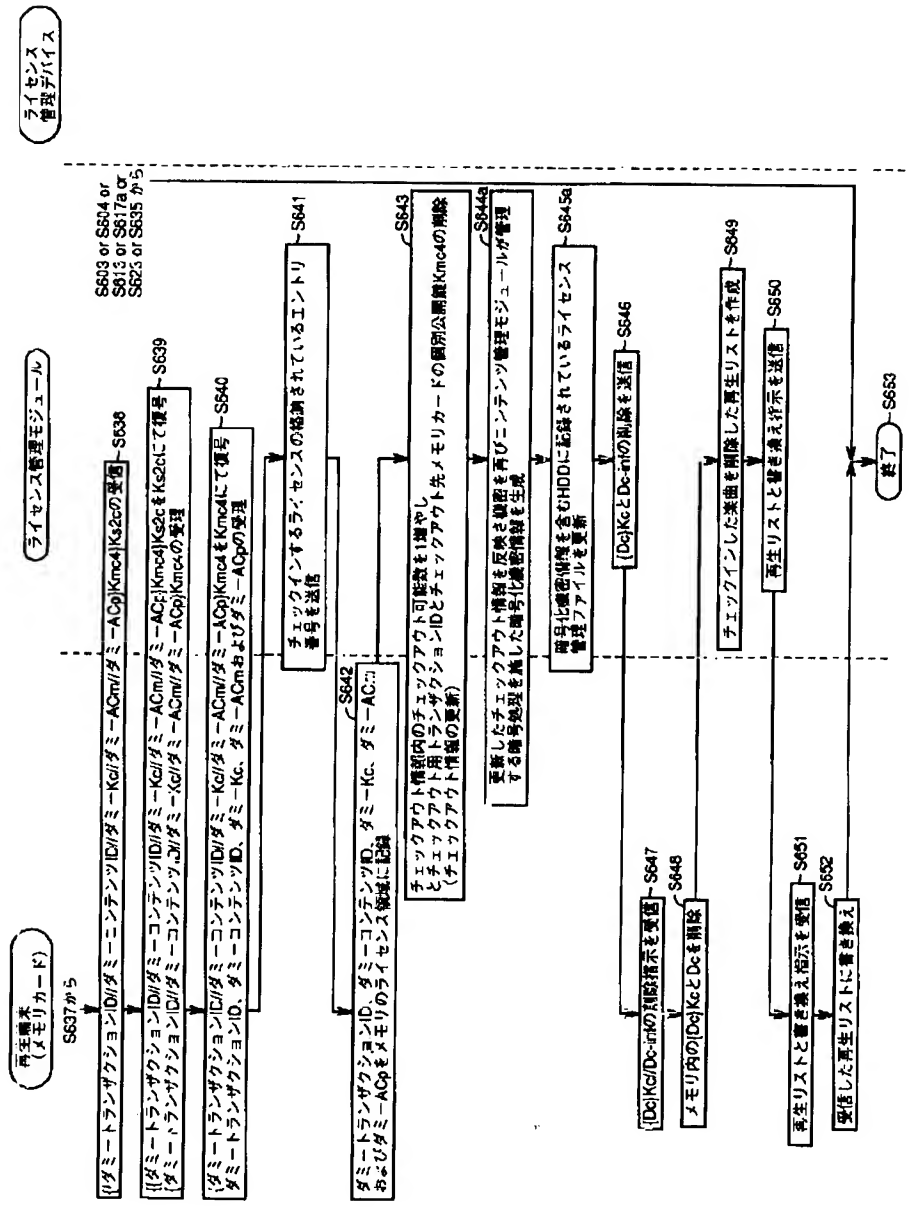
【図６５】


再生端末
(メモリカード)
ライセンス管理モジュール
ライセンス管理デバイス
S608から
S609
Ks2aをKs2にて暗号化し、{Ks2a}Ks2をライセンス管理デバイスに入力
{Ks2a}Ks2をKs2にて復号し、Ks2aを受理
S610
エントリ番号0をライセンス管理デバイスに入力
S611
エントリ番号を受信し、そこに格納されているトランザクションIDb、コンテンツIDb、Kb、ACmbおよびACpbを得る
S612
S613
ACmbの確認再生？
No
Yes
S614
KbとACpbをKs2aにて暗号化し、{Kb//ACpb}Ks2aを出力
S615
{Kb//ACpb}Ks2aをKs2aにて復号し、Kbを取得
暗号化機密ファイルをHDDより取得して、復号し格納されているKbを取得
S616a
S616b
Kbの一致？
エントリ＝機密ファイル
No
Yes
ライセンス管理ファイルの機密情報を復号して機密情報（トランザクションID、コンテンツID、Kc、ACm、ACp、チェックアウト情報およびバインディング情報）を取得
S617a
認証データ送信要求の送信
S618
認証データ送信要求の受信
S619
{KPm3//Cm3}KPa送信
S620
{KPm3//Cm3}KPaの受信
S621
{KPm3//Cm3}KPaをKPaにて復号
S622
S623
KPm3の受理
No
Yes
S624へ
S652へ

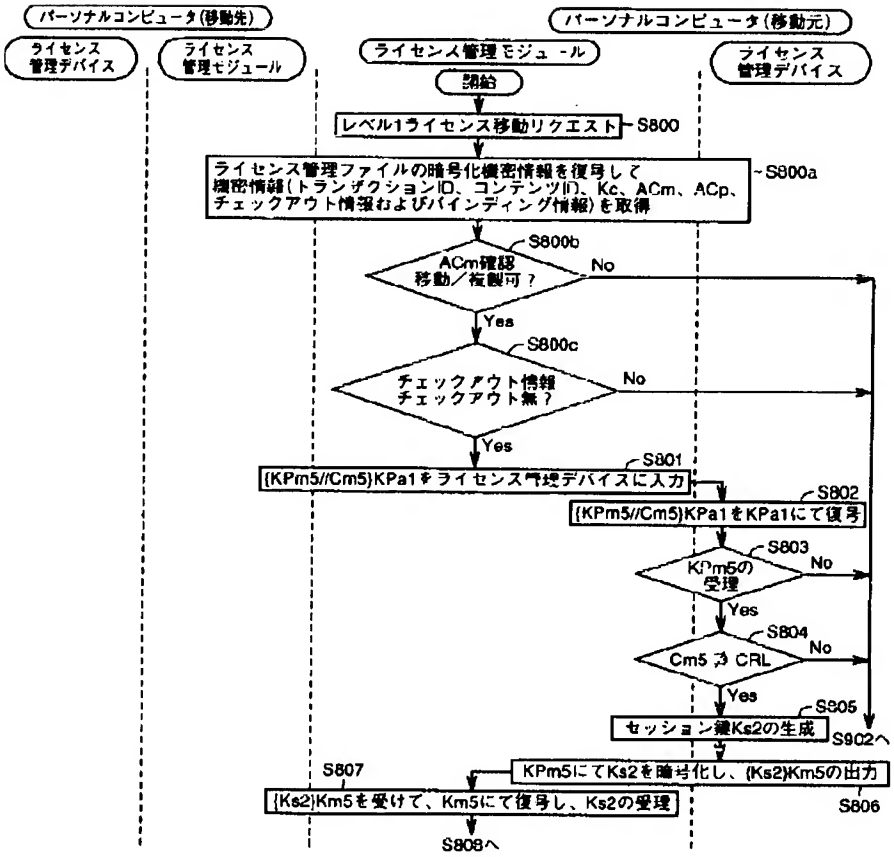
【図66】


ライセンス管理デバイス
ライセンス管理モジュール
再生端末
(メモリカード)
S623から
ダミートランザクションIDを生成
S624
セッション鍵Ks2bの生成
S625
KPm3にてKs2bを暗号化し、{Ks2b}Km3の生成
S626
ダミートランザクションID//{Ks2b}Km3の送信
S627
ダミートランザクションID//{Ks2b}Km3の受信
S628
{Ks2b}Km3を受けて、Km3にて復号し、Ks2bの取得
S629
セッション鍵Ks2cの生成
S630
メモリ内のCRLからCRLdateを取得
S631
Ks2c、KPmc4とCRLdateをKs2bにて暗号化し、
{Ks2c//KPmc4//CRLdate}Ks2bの送信
S632
{Ks2c//KPmc4//CRLdate}Ks2bを受信
S633
{Ks2c//KPmc4//CRLdate}Ks2bをKs2bにて復号し、
Ks2cおよびKPmc4の取得
S634
KPmc4ヨチェック
アウト先
S635
No
Yes
S636
ダミートランザクションID、ダミーコンテンツID、ダミーKc、ダミーACmおよびダミーACpをKmc4にて暗号化し、
{ダミートランザクションID//ダミーコンテンツID//ダミーKc//ダミーAC::}//ダミーACp}Kmc4を生成
S637
{ダミートランザクションID//ダミーコンテンツID//ダミーKc//ダミーACm//ダミーACp}Kmc4をKs2cにて暗号化し、
{{ダミートランザクションID//ダミーコンテンツID//ダミーKc//ダミーAC::n//ダミーACp}Kmc4}Ks2cの送信
S638へ
S652へ

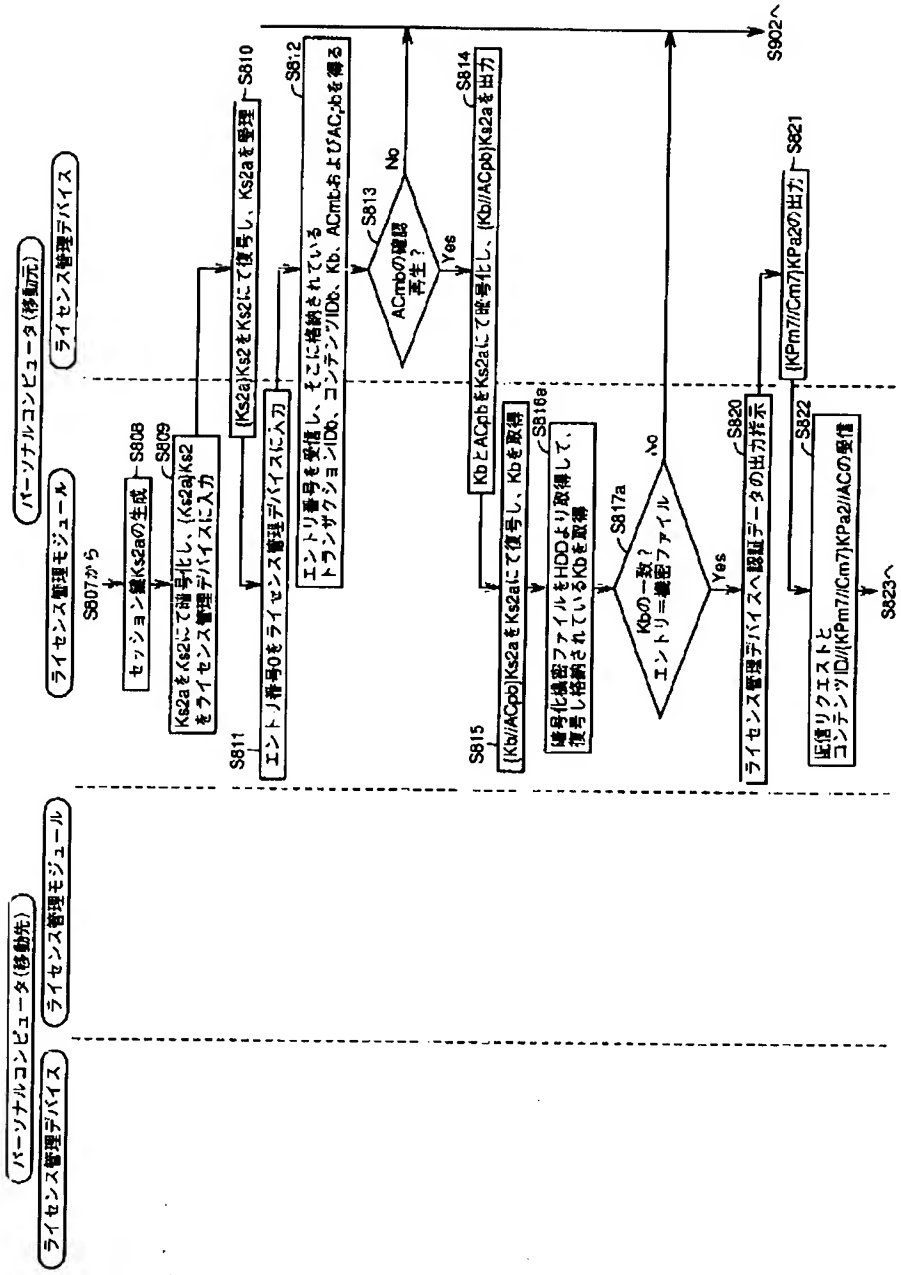
【図67】


再生機器
(メモリカード)
S637から
ライセンス管理モジュール
ライセンス
管理デバイス
S603 or S604 or
S613 or S617a or
S625 or S635 から
{{ダミートランザクションID//ダミーコンテンツID//ダミー-Kd//ダミー-ACm//ダミー-ACp}Kmc4}Ks2cの受信
S638
{{ダミートランザクションID//ダミーコンテンツID//ダミー-Kd//ダミー-ACm//ダミー-ACp}Kmc4}Ks2cをKs2cにて復号
S639
{ダミートランザクションID//ダミーコンテンツID//ダミー-Kd//ダミー-ACm//ダミー-ACp}Kmc4の管理
S640
{ダミートランザクションID//ダミーコンテンツID//ダミー-Kd//ダミー-ACm//ダミー-ACp}Kmc4をKmc4にて復号
ダミートランザクションID、ダミーコンテンツID、ダミー-Kc、ダミー-ACmおよびダミー-ACpの管理
チェックインするライセンスの格納されているエントリ番号を送信
S641
ダミートランザクションID、ダミーコンテンツID、ダミー-Kc、ダミー-AC...
およびダミーACpをメモリのライセンス格納に記録
S642
チェックアウト情報内のチェックアウト可能数を1増やし
とチェックアウト用トランザクションIDとチェックアウト先メモリカードの個別公開鍵Kmc4の削除
(チェックアウト情報の更新)
S643
更新したチェックアウト情報を反映させ鍵情報を再びコンテンツ管理モジュールが管理
する暗号処理を施した暗号化鍵情報を生成
S644a
暗号化鍵情報を含むHDDに記録されているライセンス管理ファイルを更新
S645a
{Dc}Kcと Dc-inの削除を送信
S646
{Dc}Kc//Dc-inの削除指示を受信
S647
メモリ内の{Dc}KcとDcを削除
S648
チェックインした楽曲を削除した再生リストを作成
S649
再生リストと書き換え指示を送信
S650
再生リストと書き換え指示を受信
S651
受信した再生リストに書き換え
S652
終了
S653

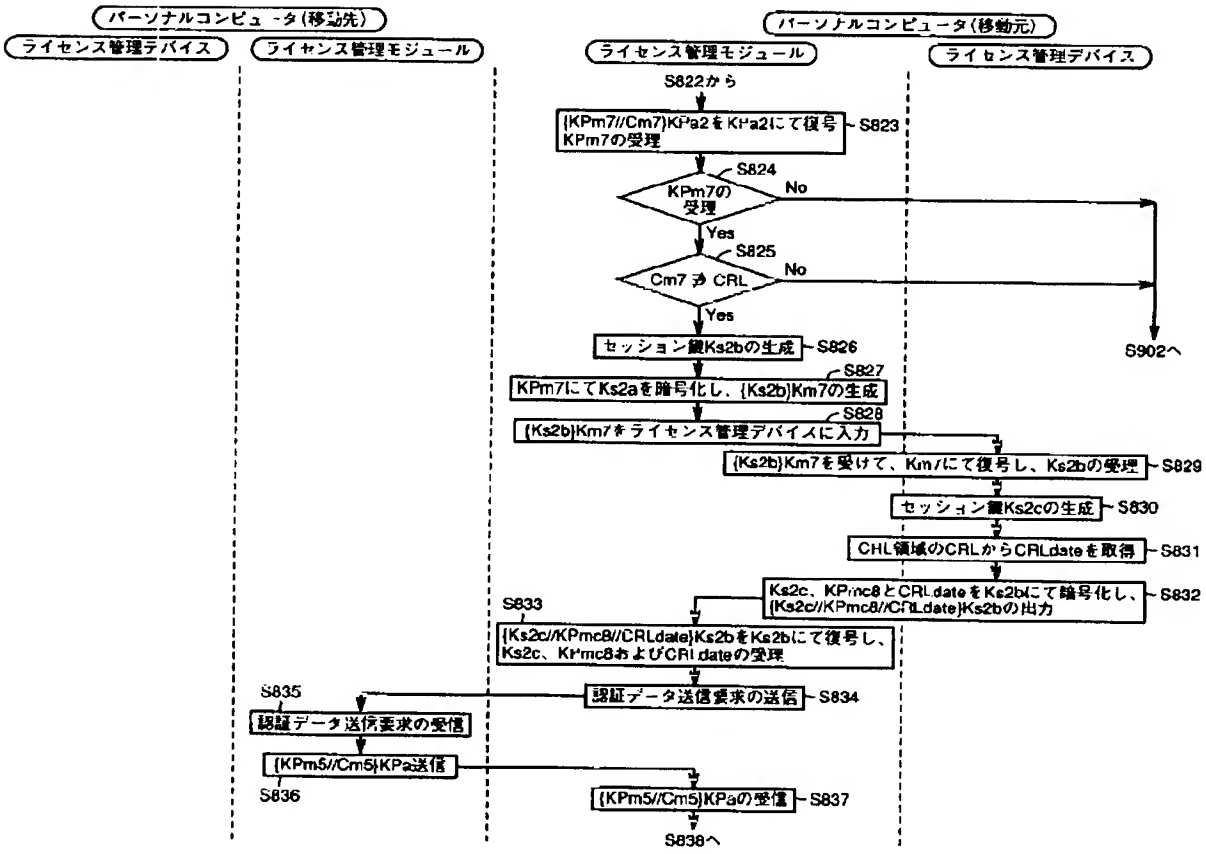
【図68】


パーソナルコンピュータ(移動先)
ライセンス管理デバイス
ライセンス管理モジュール
ライセンス管理モジュール
開始
パーソナルコンピュータ(移動元)
ライセンス管理デバイス
レベル1ライセンス移動リクエスト
S800
ライセンス管理ファイルの暗号化機密情報を復号して機密情報(トランザクションID、コンテンツID、Kc、ACm、ACp、チェックアウト情報およびバインディング情報)を取得
S800a
S800b
ACm鍵は移動／複製可？
No
Yes
S800c
チェックアウト情報はチェックアウト無？
No
Yes
S801
{KPm5//Cm5}KPa1をライセンス管理デバイスに入力
S802
{KPm5//Cm5}KPa1をKPa1にて復号
S803
KPm5の受理
No
Yes
S804
Cm5がCRL
No
Yes
S805
セッション鍵Ks2の生成
S902へ
S807
KPm5にてKs2を暗号化し、{Ks2}Km5の出力
S806
{Ks2}Km5を受けて、Km5にて復号し、Ks2の受理
S808へ

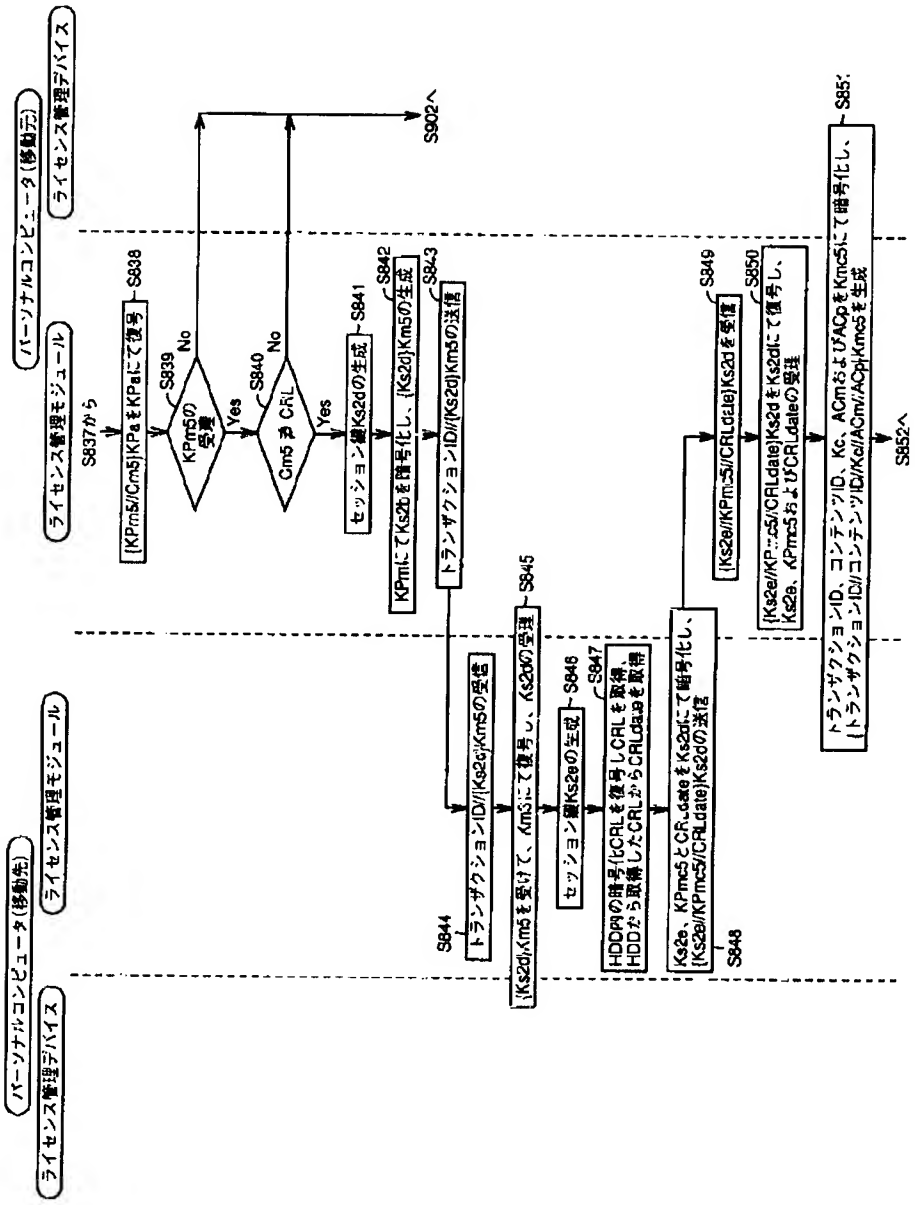
【図69】


パーソナルコンピュータ(移動先)
ライセンス管理デバイス
ライセンス管理モジュール
パーソナルコンピュータ(移動元)
ライセンス管理デバイス
ライセンス管理モジュール
S807から
S808
セッション鍵Ks2aの生成
S809
Ks2aをKs2にて暗号化し、{Ks2a}Ks2をライセンス管理デバイスに入力
S810
{Ks2a}Ks2をKs2にて復号し、Ks2aを管理
S811
エントリ番号0をライセンス管理デバイスに入力
S812
エントリ番号を受信し、そこに格納されているトランザクションID0、Kb、ACmtbおよびAC,tbを得る
S813
ACmtbの確認再生?
No
Yes
S814
KbとACpbをKs2aにて暗号化し、{Kb//ACpb}Ks2aを出力
S815
{Kb//ACpb}Ks2aをKs2aにて復号し、Kbを取得
S816a
暗号化機密ファイルをHDDより取得して、復号し格納されているKbを取得
S817a
Kbの一致?
エントリ=機密ファイル
No
Yes
S820
ライセンス管理デバイスへ認証データの出力指示
S821
{KPm7//Cm7}KPa2の出力
S822
証書リクエストとコンテンツID//{KPm7//Cm7}KPa2//ACの受信
S823へ
S902へ

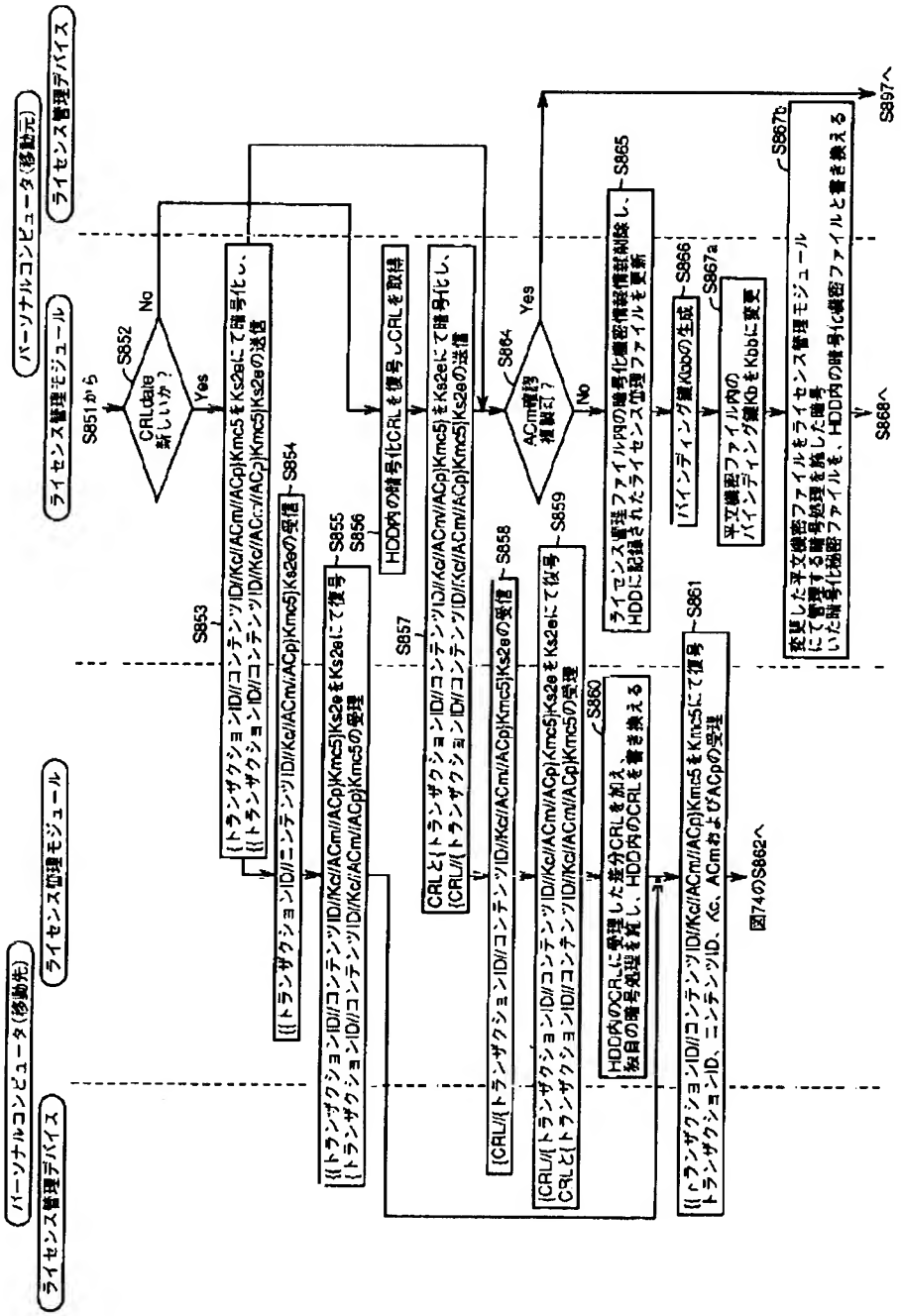
【図70】


パーソナルコンピュータ(移動先)
ライセンス管理デバイス
ライセンス管理モジュール
パーソナルコンピュータ(移動元)
ライセンス管理モジュール
ライセンス管理デバイス
S822から
{KPm7//Cm7}KPa2をKPa2にて復号
KPm7の受理
S823
S824
KPm7の受理
No
Yes
S825
Cm7 ≠ CRL
No
Yes
セッション鍵Ks2bの生成
S826
S902へ
S827
KPm7にてKs2aを暗号化し、{Ks2b}Km7の生成
S828
{Ks2b}Km7をライセンス管理デバイスに入力
{Ks2b}Km7を受けて、Kmにて復号し、Ks2bの受理
S829
セッション鍵Ks2cの生成
S830
CHL領域のCRLからCRLdateを取得
S831
Ks2c、KPmc8とCRLdateをKs2bにて暗号化し、
{Ks2c//KPmc8//CRLdate}Ks2bの出力
S832
S833
{Ks2c//KPmc8//CRLdate}Ks2bをKs2bにて復号し、
Ks2c、KPmc8およびCRLdateの受理
S835
認証データ送信要求の送信
S834
認証データ送信要求の受信
{KPm5//Cm5}KPa送信
S836
{KPm5//Cm5}KPaの受信
S837
S838へ

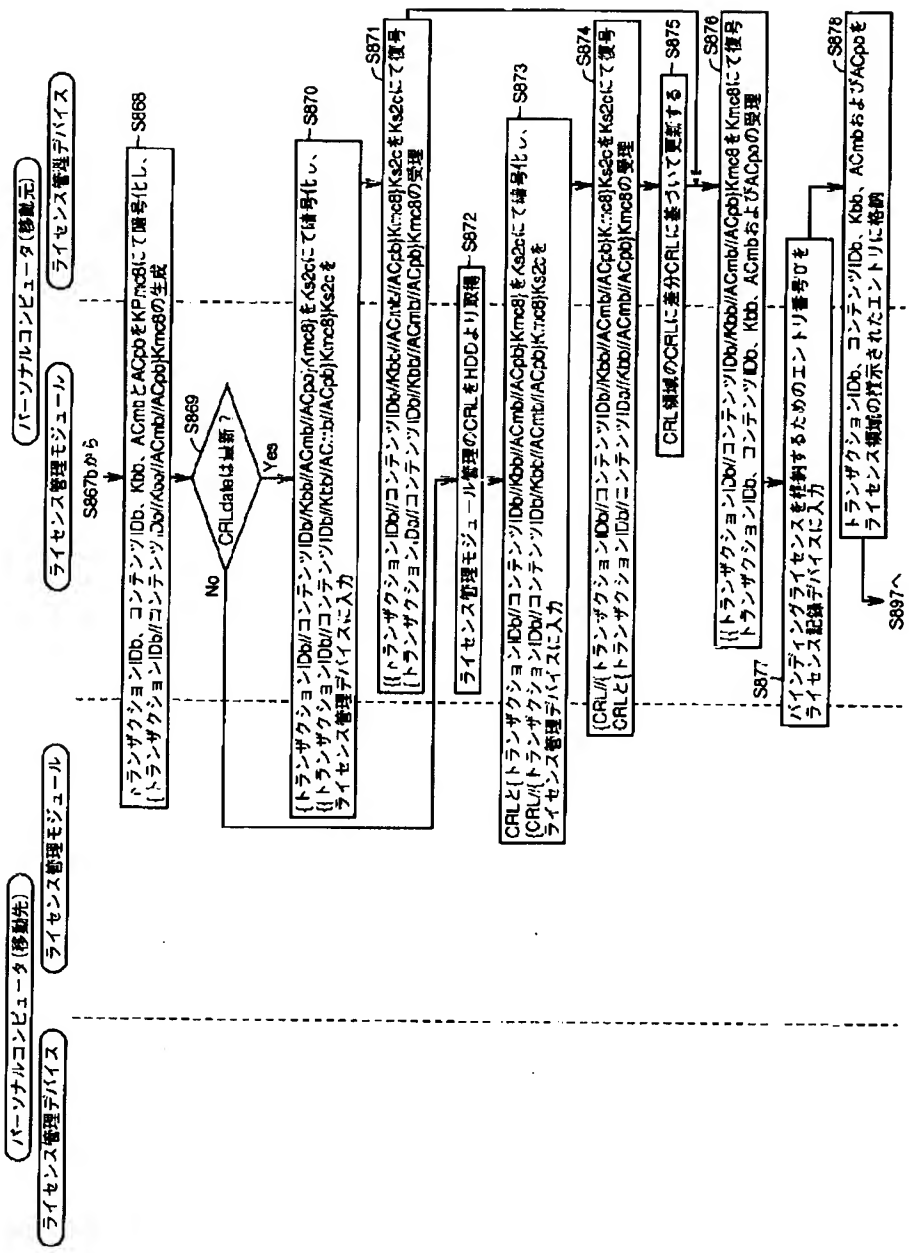
【図71】


パーソナルコンピュータ(移動先)
ライセンス管理デバイス
ライセンス管理モジュール
パーソナルコンピュータ(移動元)
ライセンス管理モジュール
ライセンス管理デバイス
S837から
{KPm5//Cm5}KPaをKPaにて復号
S838
KPm5の受理
S839
No
Yes
S840
No
Cm5 ≠ CRL
Yes
セッション鍵Ks2dの生成
S841
KPmにてKs2bを暗号化し、{Ks2d}Km5の生成
S842
トランザクションID//{Ks2d}Km5の送信
S843
S902へ
S844
トランザクションID//{Ks2d}Km5の受信
{Ks2d}Km5を受けて、Km5にて復号し、Ks2dの受理
S845
セッション鍵Ks2aの生成
S846
HDDからCRLdateを取得
S847
Ks2a、KPmc5とCRLdateをKs2dにて暗号化し、
{Ks2a//KPmc5//CRLdate}Ks2dの送信
S848
{Ks2a//KPmc5//CRLdate}Ks2dを受信
S849
{Ks2a//KPmc5//CRLdate}Ks2dをKs2dにて復号し、
Ks2a、KPmc5およびCRLdateの受理
S850
トランザクションID、コンテンツID、Kc、ACmおよびACpをKmc5にて暗号化し、
{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc5を生成
S851
S852へ

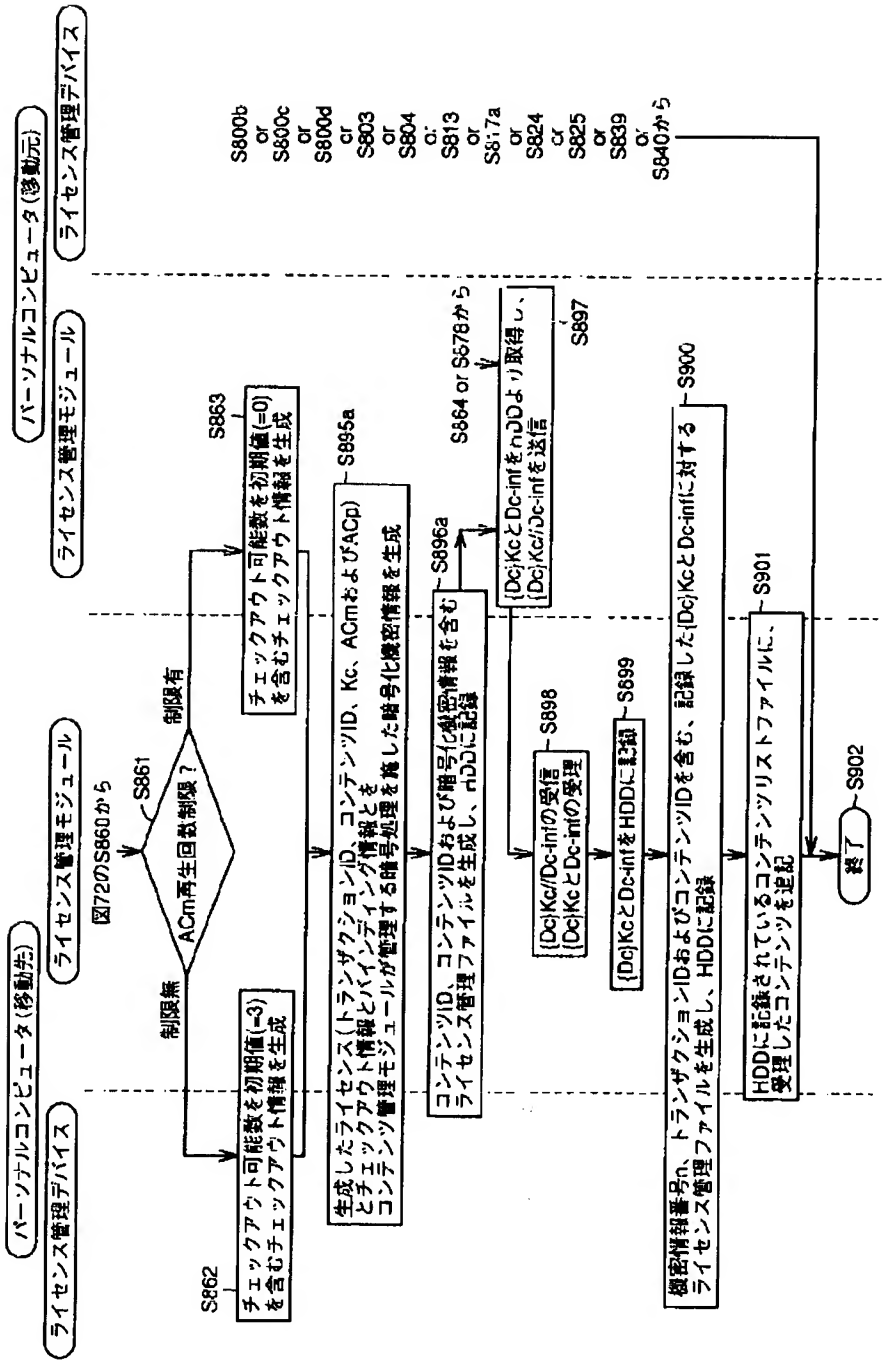
【図72】


パーソナルコンピュータ(移動先)
ライセンス管理デバイス
ライセンス管理モジュール
パーソナルコンピュータ(移動元)
ライセンス管理モジュール
ライセンス管理デバイス
S851から
S852
CRLdateは新しいか？
No
Yes
S853
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc5をKs2aにて暗号化し、
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc5}Ks2aの送信
{{トランザクションID//ニンテンツID//Kc//ACm//ACp}Kmc5}Ks2aの受信
S854
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc5}Ks2aにて復号
S855
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc5}Ks2aをKs2aにて復号
S856
HDD内の暗号化CRLを復号しCRLを取得
S857
CRLと{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc5}をKs2eにて暗号化し、
{CRL//{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc5}Ks2eの送信
{CRL//{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc5}Ks2aの受信
S858
S864
ACm情報は復旧？
Yes
No
S859
{CRL//{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc5}Ks2eにて復号
CRLと{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc5}Ks2aをKs2eにて復号
S860
HDD内のCRLに登録した差分CRLを加え、
最新の暗号処理を探し、HDD内のCRLを書き換える
S865
ライセンス管理ファイル内の暗号化機密情報情報削除し、
HDDに記録されたライセンス管理ファイルを更新
S866
バインディング鍵Kabの生成
S867a
平文機密ファイル内の
バインディング鍵KbをKabに変更
S867b
S868へ
S897へ
S861
{{トランザクションID//コンテンツID//Kc//ACm//ACp}Kmc5をKmc5にて復号
トランザクションID、ニンテンツID、Kc、ACmおよびACpの受理
図74のS862へ
変更した平文機密ファイルをライセンス管理モジュール
にて管理する暗号処理を施した暗号
いた暗号化機密ファイルも、HDD内の暗号化機密ファイルと書き換える

【図73】


パーソナルコンピュータ(移動先)
ライセンス管理デバイス
ライセンス管理モジュール
パーソナルコンピュータ(移動元)
ライセンス管理モジュール
ライセンス管理デバイス
S867bから
S868
{トランザクションIDb、コンテンツIDb、Kbb、ACmbとACpbをKPmc8にて暗号化し、
{トランザクションIDb//コンテンツIDb//Kbb//ACmb//ACpb}Kmc8の生成
S869
CRLdataは最新?
No
Yes
S870
{トランザクションIDb//コンテンツIDb//Kbb//ACmb//ACpb}Kmc8をKs2cにて暗号化し、
{{トランザクションIDb//コンテンツIDb//Kbb//ACmb//ACpb}Kmc8}Ks2cを
ライセンス管理デバイスに入力
S871
{{トランザクションIDb//コンテンツIDb//Kbb//ACmb//ACpb}Kmc8}Ks2cを
{{トランザクションIDb//コンテンツIDb//Kbb//ACmb//ACpb}Kmc8}Ks2cにて復号
S872
ライセンス管理モジュール管理のCRLをHDDより取得
S873
CRLと{{トランザクションIDb//コンテンツIDb//Kbb//ACmb//ACpb}Kmc8}をKs2cにて暗号化し、
{CRL//{{トランザクションIDb//コンテンツIDb//Kbb//ACmb//ACpb}Kmc8}Ks2c}を
ライセンス管理デバイスに入力
S874
{CRL//{{トランザクションIDb//コンテンツIDb//Kbb//ACmb//ACpb}Kmc8}Ks2cを
CRLと{{トランザクションIDb//コンテンツIDb//Kbb//ACmb//ACpb}Kmc8}Ks2cにて復号
S875
CRL領域のCRLに基づいて更新する
S876
{{トランザクションIDb//コンテンツIDb//Kbb//ACmb//ACpb}Kmc8をKmc8にて復号
トランザクションIDb、コンテンツIDb、Kbb、ACmbおよびACpbの受理
S877
バインディングライセンスを格納するためのエントリ番号Oを
ライセンス記録デバイスに入力
S878
トランザクションIDb、コンテンツIDb、Kbb、ACmbおよびACpbを
ライセンス領域の指示されたエントリに格納
S897へ

【図74】



フロントページの続き

(51)Int.Cl.[7]	識別記号	FI		(参考)
		H04L 9/00	601E	
			675B	

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(71)出願人　000004167
日本コロムビア株式会社
東京都港区赤坂４丁目14番14号
(72)発明者　堀　吉宏
大阪府守口市京阪本通２丁目５番５号　三洋電機株式会社内
(72)発明者　上村　透
大阪府守口市京阪本通２丁目５番５号　三洋電機株式会社内
(72)発明者　畠山　卓久
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　高橋　政孝
石川県河北郡宇ノ気町字宇野気ヌ98番地の２　株式会社ピーエフユー内
(72)発明者　常広　隆司
神奈川県横浜市戸塚区吉田町292番地　株式会社日立製作所システム開発研究所横浜ラボラトリ内
(72)発明者　大森　良夫
神奈川県川崎市川崎区港町５番１号　日本コロムビア株式会社川崎工場内

Ｆターム(参考)　5J104 AA07 AA13 AA15 AA16 EA06
EA19 KA02 KA05 NA02 NA03
NA06 NA35 NA37 NA38 NA41
NA42 PA07 PA11